PERSONAL ANONYCLOUD

Departamento de Arquitectura de Computadores y Automática.
Facultad de Informática
Universidad Complutense de Madrid
Proyecto de Sistemas Informáticos
Curso
2014/2015

Autores:
Sergio Baños Rodríguez
Alberto González Vicente
Alba Moragrega Sánchez

Directores:
José Luis Vázquez Poletti
José Manuel Velasco Cabo

Dedicatoria

Alberto González

A mi familia, en especial a mis padres, por el apoyo, el esfuerzo y por hacer de mi lo que soy.

A FDICore, por la falta de gol, la falta de apoyo en larga y por los dropboxs. Por las fiestas en casa de "Quique", por la sabiduría adquirida en la RITSI, las tardes en paraninfo y las noches en Cats.

A mis amigos, por el BOT, por Lozoya, por el Jarra, por las salidas en bici y las desconexiones tan necesarias en determinadas épocas. Por permitirme ser parte de ellos.

A Celia, por el poquito a poco, por enseñarme a estudiar y por regalarme sonrisas a cambio de nada.

A todos aquellos maestros, que a su cargo le pusieron por nombre profesor. Del colegio a la Universidad.

A mi antiguo yo, por superarme.

*^^*

Alba Moragrega

A mis padres, Isabel y Rafael, porque gracias a vosotros y a vuestro enorme esfuerzo he llegado donde estoy ahora, por apoyarme y animarme siempre que he perdido las fuerzas, por no dejar que me rindiese nunca y por hacerme ver que podía conseguir llegar hasta aquí.

A mi hermana, Noelia, por animarme, ayudarme siempre y por nuestros buenos momentos.

A mi abuelo, Juan José, por no haberte dedicado todo el tiempo que me hubiese gustado cuando vienes a vernos y siempre contarnos chistes, y a mi abuela Pilar, que en paz descanse, porque estaría muy orgullosa de ver donde ha llegado su nieta.

A mi novio, Alberto Martín, por tus sabios consejos y ayudarme siempre que lo he necesitado, por animarme en los malos momentos y sacarme siempre una sonrisa, por aguantar mi mal humor y desesperación cuando algo no me salía bien, por recordarme siempre que todo esfuerzo tiene su recompensa y que todo se puede conseguir, por cuidarme y preocuparte siempre por mí, por estar a mi lado y por hacerme cada día más feliz.

A mis amigos de la facultad, porque gracias a vosotros ha sido más llevadero el paso por la universidad.

Sergio Baños

Sin duda, mi dedicatoria va a mis dos familias: a la que no se elige y a la se elige.

La que no se elige, pero no cambiaría por todo el oro del mundo. A mi madre, por enseñarme lo que es la superación desde que tengo uso de razón, y cuanta más razón tengo más lo descubro. A mi Padre, por enseñarme que rectificar es más valiente y útil que el orgullo. A mis hermanos: Jorge, por no importarle las horas de sueño que le robaba para llegar a este proyecto (nadie aguanta la luz por la noche como él). María, por darme su tiempo para que yo aprovechase el mío, sabiendo siempre lo que necesitaba. Pedro, sin estar ya tan cerca, conseguía que no lo pareciese; siempre estuvo ahí antes de que pudiera llamarle. Y lo más importante, por quererme, cuidarme y apoyarme, cuando no siempre es fácil.

La que se elige, por permitirme crecer con ella:

Con los que llevo creciendo desde que el babi era mi uniforme de guerra. Con vosotros he compartido tanto y tan grande que necesitaría otro cuaderno para daros las gracias. Sin duda parte de lo que soy y seré os lo debo a vosotros. Aún sin saberlo fuiste la fuente de autoestima cuando más faltaba, y el abrazo que necesite en todo momento bajo. Espero seguir dedicando trabajos en un futuro, y que estéis en esas dedicatorias, o por qué no, que las hagamos juntos.

A los más "nuevos", mi núcleo duro y sus nuevos miembros; cómo pasa el tiempo, parece que fue ayer cuando nos mirábamos para ver si nos presentábamos, y hoy no nos hace falta mirarnos para saber que pensamos. Nadie lucirá nuestro rosa con más clase y show que nosotros, nadie dejará su huella por la península y más allá como nosotros, y nadie construirá sagas nocturnas como las que hemos vivido y convertir la casa de Enrique en biblioteca nacional).Y sí, la facultad, lo que hemos pasado allí, lo bueno, malo y peor será algo que nos una para siempre.

Sería injusto olvidarme de la persona con la que fuimos 4 como Los Platero, pero paró el tren. A las dos personas que me quisieron y más he querido. Aunque no están en el punto final han sido fundamentales para llegar a él y la motivación que me hizo continuar. Gracias Susana y Carmela. Tatiana, gracias por entenderme como si hubieses vivido exactamente lo que yo. A las Torrenses, que nos sigamos peleando. Sin olvidar a mi "familia verde", por espabilarme, preocuparse por mí, hacerme pasar un turno que creía imposible como un rato increíble y mantenerme los pies en el suelo. Gonzalito, mi media familia verde y amigo, muchas gracias por todo.

Por último, agradecer a mi profesor Daniel el enseñarme a pensar y preguntarme, ¿por qué?, y no repetir y asumir. Sin duda marcó un antes y después para mí.

Y por mí, porque al final lo he conseguido

Agradecimientos

Gracias a la Universidad Complutense de Madrid, en concreto a la Facultad de Informática por habernos hecho sufrir hasta lograr aprender.

Agradecer en especial a nuestros directores de proyecto, José Luis Vazquez-Poletti y José Manuel Velasco Cabo , por su ayuda, paciencia y por orientarnos en la realización de este proyecto.

Tabla de contenido

Índice de Figuras

Índice de abreviaturas

Abreviatura	Descripción
PA	Personal Anonycloud
VPN	Virtual Private Network
PPTP	Point-to-Point Tunneling Protocol
MPPE	Microsoft Point-to-Point Encryptation
L2TP	Layer 2 Tunneling Protocol
L2TPv3	Layer 2 Tunneling Protocol versión 3
IPsec	Internet Protocol security
DES	Data Encryption Standard
Triple DES	Triple cifrado del DES
BYOD	Bring Your Own Device
SSL	Secure Sockets Layer
NAT	Network Address Translation
HTTPS	HyperText Transfer Protocol Secure
IP L3	IP Layer 3
GPL	General Public License
TCP	Transmission Control Protocol
FDB	Forwarding DataBase
UDP	User Datagram Protocol
DNS	Domain Name System
DDNS	Dynamic DNS
SSTP	Secure Socket Tunneling Protocol
ICMP	Internet Control Message Protocol
TLS	Transport Layer Security
LAN	Local Area Network
OSI	Open System Interconnection
IEEE	Institute of Electrical and Electronics Engineers
IEEE 802.11	Estándar que define el uso de los dos niveles inferiores de la arquitectura OSI
PYME	Pequeña y Mediana Empresa
IANA	Internet Assigned Numbers Authority
TOR	The Onion Router
ISP	Internet Service Provider
VoIP	Voice over IP
SSH	Secure Shell
SSH2	Secure Shell versión 2
VNC	Virtual Network Computing
SFTP	Secure File Transfer Protocol
FTP	File Transfer Protocol
DMZ	Demilitarized zone
MAC	Media Access Control

NIST	National Institute of Standards and Technology
IAAS	Infrastructure as a Service
PAAS	Platform as a Service
SAAS	Software as a Service
SIG o GIS	Sistema de Información Geográfica (GIS en Inglés, Geographic Information System)
BSD	Licencia BSD (Berkeley Software Distribution)
RSA	Sistema criptográfico (Rivest, Shamir y Adleman)
JSCH	Java Secure Channel
SDK	Software Development Kit

Resumen

Personal AnonyCloud es un proyecto que soluciona varios de los principales problemas en redes hoy en día. Por una parte, actualmente las herramientas VPN solo permiten conexiones punto a punto, es decir, cliente a servidor. Con PA podremos conseguir una red VPN compuesta por varios terminales de repetición y por otro lado aumentar la seguridad, debido a que los terminales son propios.

Estas máquinas serán creadas bajo demanda en servicios cloud públicos generales, siendo reemplazadas en caso de cualquier tipo de intrusión.

Además, PA ofrece una interfaz intuitiva y simple, permitiendo el uso de la herramienta a cualquier persona, sea cual sea su nivel de conocimiento sobre servicios VPN

Palabras clave: *Seguridad, Computación, Nube, VPN, SSH, SoftEther, ArcGIS, Automatización, Geolocalización, túnel.*

Abstract

Personal AnonyCloud is a project that attempts to resolve some of major problems within the networks nowadays. On the one hand, VPN tools only allow point to point connections, i.e., from client to server. With PA software we will be able to build a VPN network composed of some relay servers, also enables us to increase the network´s security, because we are the terminal owners.

These machines will be created on demand at general public cloud services, being replaced in case of any type of intrusion.

Besides, PA offers an intuitive and simple interface, allowing someone the use of the tool someone, regardless of their level of knowledge about VPN services.

Keywords: *Cloud Computing, Virtual Private Network, VPN, SSH, SoftEther, ArcGIS, Script, GeoPosition, tunnel.*

1. Introducción

Actualmente una de las mayores dificultades que nos encontramos en una empresa o que se encuentra cualquier usuario al implantar y mantener una red local de ordenadores es la seguridad. Dentro de la red es una tarea que puede ser realizada sin grandes dificultades, ya que el usuario posee el control del tráfico y la posibilidad de supervisarlo en su totalidad.

El mayor quebradero de cabeza comienza cuando una empresa intenta desarrollarse en este mundo globalizado y abrir unas oficinas en la ciudad más importante de su país, o quien sabe, un nuevo grupo de trabajo en una localización remota en la que sus trabajadores producen y trabajan mejor. ¿Qué hacemos para conectar nuestra sede central con estas pequeñas sucursales y viceversa?

Supongamos que la central posee un gran número de ordenadores en los cuales se encuentra la información básica de la empresa y a la cuál toda sucursal está interesada en acceder ante la mínima gestión que realicen. ¿Dónde está ahora la seguridad? ¿Sigue siendo tan fácil?

La única solución es poner la mochila a nuestros datos y mandarlos a viajar por el extenso mundo que es Internet, sin control sobre el tráfico una vez que salgan al exterior y antes de que lleguen a nuestra oficina de destino, entonces nuestra información estará disponible públicamente en internet para todo aquel que desee y sepa buscarla. Obviamente este es un riesgo que ninguna empresa ni ningún usuario están dispuesto a asumir.

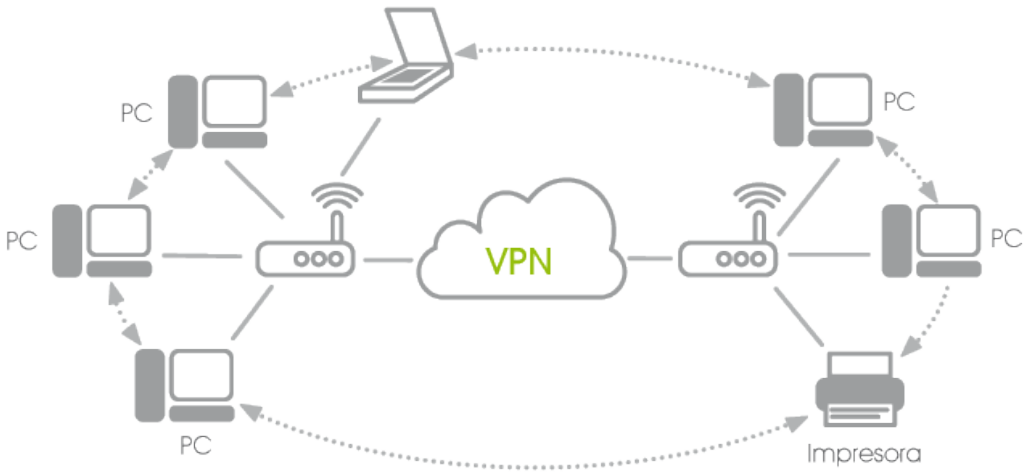

Figura 1 Virtual Private Network

Cabe destacar, un menor grupo de usuarios que utiliza software para acceder a información en otras localizaciones, debido a las restricciones de sus países en cuanto al acceso a la información, gracias al enmascaramiento IP.

Por suerte existe la tecnología Virtual Private Network (VPN, desde este punto). A grandes rasgos, esta tecnología nos permite crear redes locales entre distintas localizaciones, con una gran seguridad y reduciendo los costes de un cableado físico.

El uso de la tecnología VPN, en estos tiempos en los que podríamos pensar que es totalmente útil para todo usuario, está casi monopolizado por empresas o instituciones, además de usuarios medianamente avanzados.

¿Por qué solo los usuarios avanzados, aquellos que tiene capacidad para trabajar sobre VPN, pueden usar esta tecnología que ayudaría a todos?

La motivación de Personal Anonycloud es hacer llegar y facilitar el uso de esta tecnología a las personas que por falta de conocimientos o de tiempo, no pueden utilizar VPN en sus operaciones y/o trabajos.

Integrando el proyecto SoftEther VPN Project, desarrollado por personal de la universidad de Tsukuba en Japón, hemos conseguido una aplicación que enmascara la dificultad técnica que pueda entrañar la instalación y configuración de un software VPN.

Figura 2 Personal AnonyCloud

A través de una interfaz, el usuario puede configurar su propio entramado de redes VPN, provistas por diferentes Servicios de Cloud, como pueden ser Amazon Web Services o Microsoft Azure.

En definitiva, un proyecto para hacer accesible a todo el mundo un nivel extra de seguridad

2. Estado del arte

2.1. Tecnología VPN

2.1.1. ¿Qué es?

Una VPN (*Virtual Private Network*) es una tecnología de red utilizada para conectar una o más computadoras a una red privada utilizando Internet. Las empresas suelen utilizar una VPN para que sus empleados desde sus casas u hoteles puedan acceder a recursos corporativos que de otro modo, no podrían. Pero VPN es algo más que esta funcionalidad. En conjunto con lo anterior, una implementación correcta de esta tecnología asegura la integridad y confidencialidad de la información.

2.1.2. ¿Cómo funciona?

A través de una VPN pasa información privada y confidencial que en las manos equivocadas, podría resultar perjudicial para cualquier empresa. Esto se agrava aún más si el empleado en cuestión se conecta utilizando un Wi-Fi público sin protección. Afortunadamente, este problema puede ser mitigado cifrando los datos que se envían y reciben. Para poder lograr este objetivo, se pueden utilizar los siguientes protocolos:

- PPTP/MPPE: tecnología desarrollada por un consorcio formado por varias empresas. PPTP soporta varios protocolos VPN con cifrado de 40 bits y 128 bits utilizando el protocolo *Microsoft Point to Point Encryption* (MPPE). **PPTP por sí solo no cifra la información**.
- L2TP/IPsec (L2TP sobre IPsec): tecnología capaz de proveer el nivel de protección de IPsec sobre el protocolo de túnel L2TP. Al igual que PPTP, **L2TP no cifra la información por sí mismo**.
- IPsec (*Internet Protocol Security*): **permite mejorar la seguridad a través de algoritmos de cifrado robustos** y un sistema de autentificación más exhaustivo. IPsec posee dos métodos de encriptado, modo transporte y modo túnel. Asimismo, soporta encriptado de 56 bits y 168 bits (triple DES).

Parte de la protección de la información que viaja por una VPN es el cifrado, no obstante, verificar que la misma se mantenga íntegra es igual de trascendental. Para lograr esto, IPsec emplea un mecanismo que si detecta alguna modificación dentro de un paquete, procede a descartarlo. Proteger la confidencialidad e integridad de la información utilizando una VPN es una buena medida para navegar en Wi-Fi públicos e inseguros incluso si no se desea acceder a un recurso corporativo.

2.1.3. Softether VPN

2.1.3.1. ¿Qué es?

SoftEther VPN (“SoftEther” significa “Software Ethernet”) es un software VPN multiprotocolo, uno de los más potentes y sencillos de usar en todo el mundo. SoftEther VPN es open source. Se puede usar para uso personal o comercial sin coste alguno.

SoftEther es una magnífica alternativa a OpenVPN y Microsoft VPN Servers. SoftEther tiene la misma funcionalidad que OpenVPN. Puedes migrar de OpenVPN a SoftEther VPN de manera muy sencilla. SoftEther VPN ofrece mayor velocidad respecto a OpenVPN. Además SoftEther VPN también soporta Microsoft SSTP VPN para Windows Vista/ 7 / 8. Ya no necesitas pagar grandes cantidades por Windows server para realizar accesos remotos por VPN.

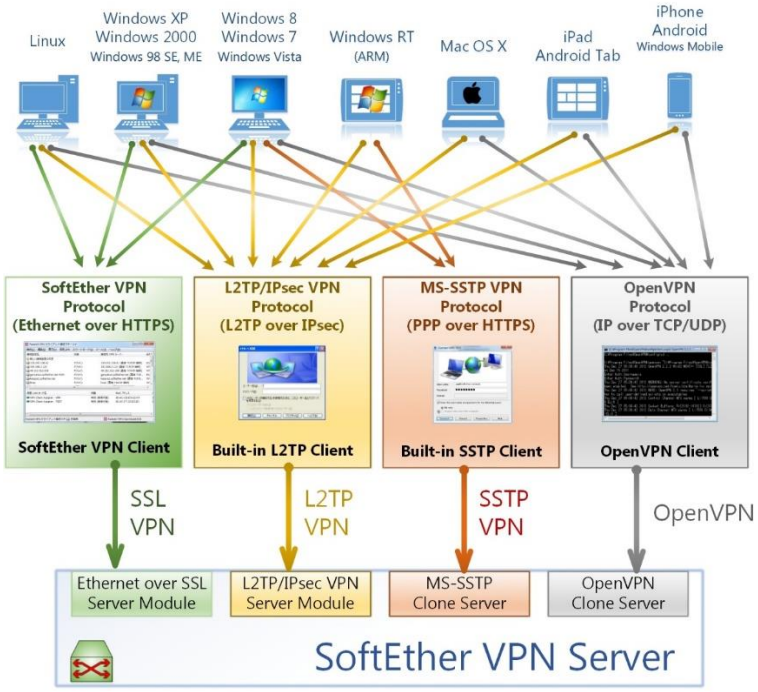

Figura 3 SoftEther VPN

SoftEther VPN puede ser utilizado para realizar BYOD (Bring your own device) en tu empresa. Si tienes un Smartphone, Tablet u ordenadores portátiles, la función SoftEther VPN’s L2TP/IPsec server podrá ayudarte a establecer el acceso remoto a tu red local. SoftEther VPN’s L2TP es fuertemente compatible con Windows, Mac, iOs y Android.

Hasta ahora hemos hablado de las características de SoftEther VPN, pero no se diferencia apenas de otros productos VPN. La diferencia principal de SoftEther VPN es su particular protocolo SSL-VPN para saltarse todo tipo de firewalls. El protocolo SSL-VPN de SoftEther VPN tiene una alta tasa de trabajo, baja latencia y resistencia a firewall. SoftEther VPN tiene una fuerte resistencia frente a firewalls nunca vista. La función incorporada NAT transversal penetra el firewall problemático de su administrador de red.

Puedes instalar tu propio servidor VPN bajo el firewall o NAT en tu compañía, y puedes llegar a contactar con este servidor VPN desde tu red privada en el trabajo u hogar, sin tener que modificar las configuraciones del firewall. Cualquier paquete intruso no detectara los paquetes que enviamos a través del túnel VPN, porque SoftEther VPN usa Ethernet bajo HTTPS para camuflar la información.

Es fácil imaginar, diseñar e implementar tu topología VPN con SoftEther VPN. Este virtualiza Ethernet a través de un software de conteo. SoftEther VPN Cliente implementa un Adaptador de red virtual y SoftEther VPN Server construye un Switch virtual. Puedes construir tanto acceso remoto a través de VPN como estrategias Site-to-Site fácilmente, como ampliación de Ethernet-based L2 VPN. Por supuesto, el tradicional enrutado IP L3 basado en VPN puede ser construido a través de SoftEther VPN.

SoftEther VPN posee una gran compatibilidad para los dispositivos más utilizados para realizar conexiones VPN. Además tiene la interoperabilidad con OpenVPN, L2TP, IPsec, EtherIP, L2TPv3, Cisco VPN Routers y clientes MS-SSTP VPN. SoftEther VPN es el único software VPN que soporta SSL-VPN, OpenVPN, L2TP, EtherIP, L2TPv3 e IPsec en un único programa.

SoftEther es un software libre, desarrollado como parte de la tesis de investigación de Daiyuu Nobori. El código está disponible bajo licencia GPL.

2.1.3.2. Arquitectura

La virtualización de los dispositivos Ethernet es la clave en la arquitectura de SoftEther VPN. Virtualiza los dispositivos Ethernet con la idea de realizar una red virtual privada y flexible, tanto para acceso remoto VPN y acceso site-to-site.

Implementa el comportamiento de adaptadores de red virtuales como un software de emulación del comportamiento de los adaptadores de redes Ethernet. Por otro lado, implementa Switch virtuales, llamado HUB virtual, como un software que simula el

comportamiento de un switch. Por último, implementa las sesiones VPN emulando el comportamiento de un cable ethernet entre el adaptador de red y el switch.

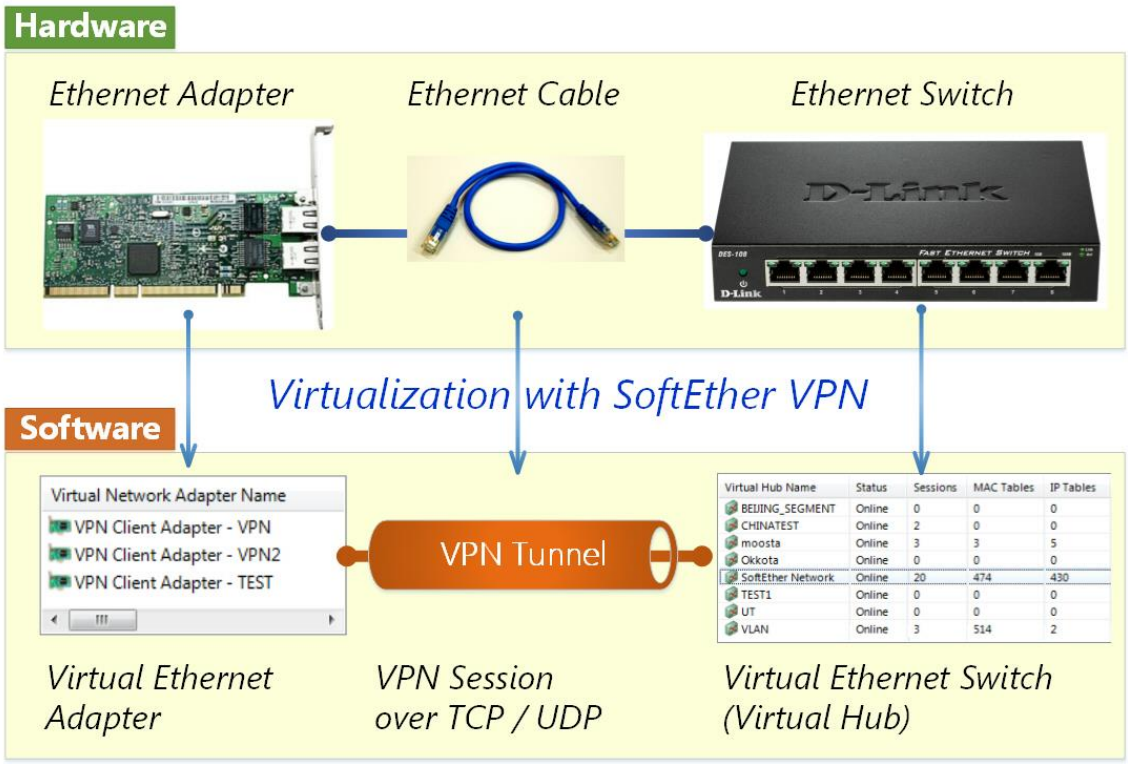

Figura 4 Virtualización con SoftEther VPN

SofEther VPN te da la posibilidad de crear varios HUB virtuales en tu servidor. Este será nuestro servidor VPN que aceptará las conexiones y peticiones desde los clientes. También se puede crear uno o varios adaptadores de red virtuales en tu terminal cliente, este ordenador será un cliente VPN, el cual establecerá la conexión con el HUB virtual del servidor VPN.
Podemos establecer sesiones VPN, llamadas túneles VPN, entre los clientes y servidores. Una sesión VPN podemos considerarla la virtualización del cable de red, la conexión se realiza sobre el protocolo TCP/IP. Las señales durante la sesión VPN son encriptadas bajo SSL. Por ello, se puede establecer una sesión VPN segura a través de internet. Una sesión VPN es establecida como “VPN sobre HTTPS”, que esto significa que podemos crear una conexión VPN más allá del tipo de firewalls and NATs.

El HUB virtual intercambia todos los paquetes procedentes de cada sesión VPN a otras sesiones conectadas. El comportamiento es el mismo que un switch tradicional. El HUB virtual posee FDB (en inglés, Forwarding DataBase) para optimizar la transmisión de los frames.
Además se puede definir un Bridge local entre el HUB Virtual y el segmento de red física usando la función de Bridge local. Esta función intercambia los paquetes entre el

adaptador de red y el HUB virtual. Puedes realizar accesos remotos desde casa o móvil a la red de tu compañía usando dicha función.

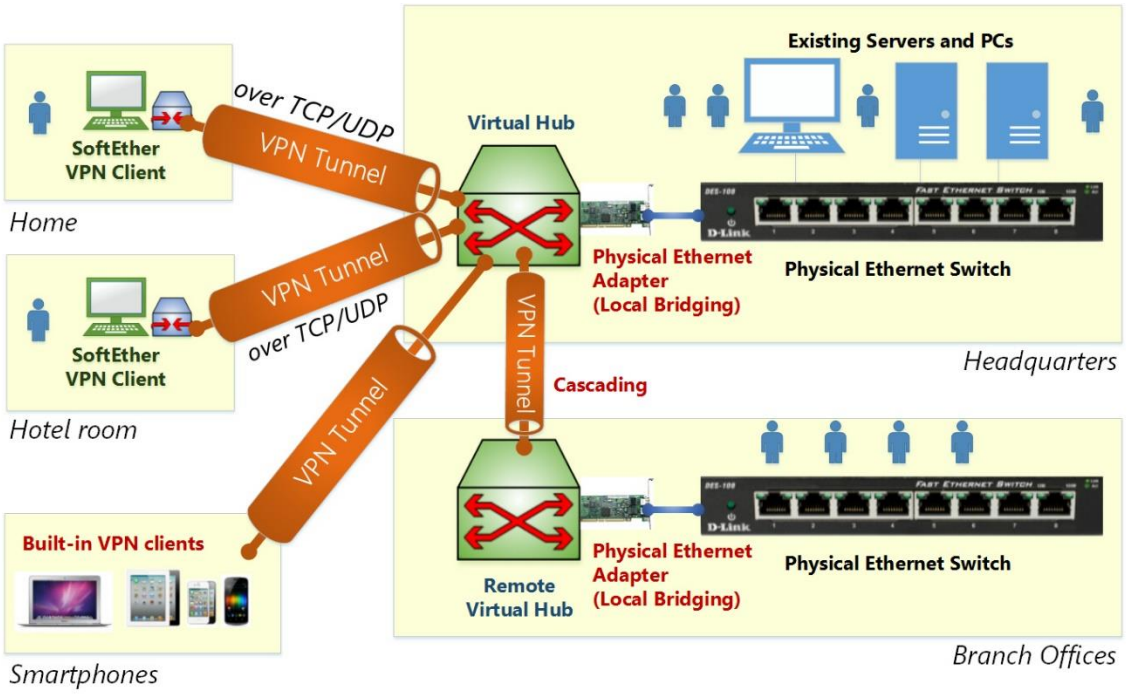

Figura 5 Arquitectura Virtual Hub

Por otro lado se encuentran las conexiones en cascada entre 2 o más HUBs virtuales. Con las conexiones en cascada podemos integrar más de un segmento Ethernet en uno solo. Por ejemplo, si creamos una conexión en cascada entre los sitios A, B y C, entonces cualquier terminal en el sitio A es capaz de comunicarse con los computadores del sitio B y el sitio C. Esto es lo que se define como conexión VPN site-to-site.

SoftEther VPN también puede establecer conexiones sobre el protocolo UDP. El modo UDP en SoftEther VPN soporta NAT transversal. Esta función permite que un servidor VPN acepte peticiones entrantes de sesiones VPN a través de NAT o firewall existentes y por tanto, no se necesitan permisos especiales para su uso. Adicionalmente, SoftEther VPN Server puede ser utilizado bajo direcciones de IP dinámicas, desde que SoftEther ha desarrollado la función Dynamic DNS (DDNS).

SoftEther VPN Servers soportan diversos protocolos VPN adicionales, incluyendo L2TP/IPsec, OpenVPN, Microsoft SSTP, L2TPv3 y EtherIP. Además de interoperabilidad en los distintos sistemas operativos móviles, para acceso como clientes VPN, y también con routers CISCO y otro vendedores de productos VPN.

2.1.3.3. VPN Azure Service

Es un servicio ofrecido a todos los usuarios de SoftEtherVPN.

Si posees tu servidor SoftEther VPN tras el NAT o el firewall y por alguna razón no puedes utilizar la función NAT Traversal, la función de DNS dinámica o VPN sobre la función ICMP/DNS puede utilizar VPN Azure. SoftEther opera VPN Azure Cloud en internet.

Tras realizar la conexión al VPN Azure, el nombre del host “example.vpnazure.net” puede ser especificado para conectar desde el servidor VPN a través de VPN Azure, a cualquier dirección IP global de uno de los proveedores cloud con los que trabaja SoftEther Corporation.

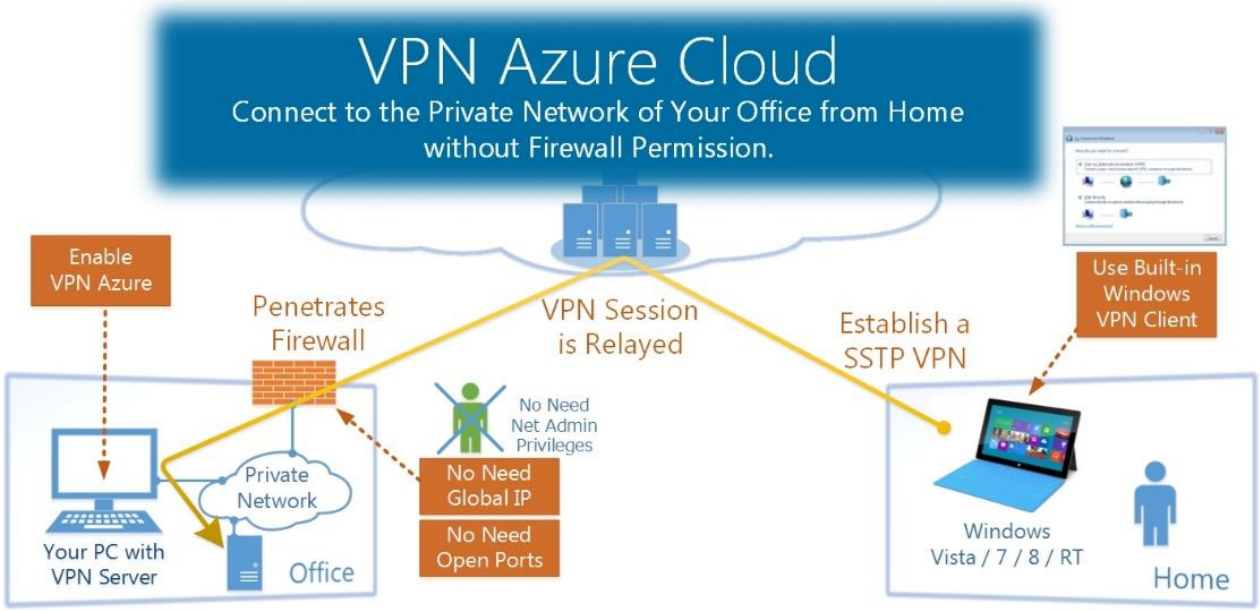

Figura 6 VPN Azure Cloud

Si un cliente VPN se conecta a un host de VPN Azure, entonces el host VPN Azure redirigirá todo el tráfico entre el cliente VPN y el servidor VPN. VPN Azure está desactivado por defecto, pero se puede activar de manera sencilla usando la herramienta de configuración de VPN Server.

2.1.4. Open VPN

OpenVPN es una solución de conectividad basada en software, una utilidad de código abierto (está publicado bajo la licencia GPL, de software libre) para soluciones SSL/TLS VPN. Fue creado por James Yonan en el año 2001 y se ha estado mejorando desde entonces. OpenVPN ofrece conectividad punto a punto con validación jerárquica de usuarios y host conectados remotamente, además de una amplia gama de configuraciones VPN basadas en SSL/TLS, incluyendo acceso remoto, LAN to LAN VPN, seguridad para Wi-Fi (redes inalámbricas bajo estándar IEEE 802.11), soluciones de balanceo de carga, respuesta ante fallos y diferentes técnicas de control de acceso. Partiendo de una premisa muy importante en los sistemas de seguridad que es: "la complejidad es el enemigo de la seguridad", OpenVPN ofrece, con un bajo coste efectivo, una alternativa a otras tecnologías VPN orientadas para las PYMEs y empresas del mercado. OpenVPN tiene asignado y reservado el puerto 1194 de manera oficial por la IANA.

La facilidad de uso de OpenVPN ha simplificado mucho la configuración de las VPN y arroja a la basura muchas de las complejidades que caracterizan a otras implementaciones de VPN, como por ejemplo, la que más se va a mencionar por su importancia e influencia en el mercado, IPSec, y ha hecho más accesible para la gente inexperta este tipo de tecnología. El modelo de seguridad de OpenVPN está basado en la arquitectura SSL/TLS, que es el estándar escogido actualmente por la industria para establecer comunicaciones seguras a través de Internet.

Un aspecto que hay que tener en cuenta durante todo el estudio con OpenVPN es que esta herramienta implementa redes seguras en la capa 2 o 3 (según el modo que utilice OpenVPN: Tunnel o Bridge) de la pila de protocolos OSI utilizando como extensión el protocolo SSL/TLS, soportando métodos de autenticación del cliente de manera flexible. Las implementaciones de SSL/TLS más conocidas hoy en día operan a través de un navegador Web (lo que se conoce como HTTPS), ya que se han implementado aproximaciones de SSL/TLS para aplicaciones en la capa de aplicación de la pila OSI (capa 7). Pero hay que tener muy en cuenta que este tipo de implementación Web con SSL/TLS no es una VPN y que OpenVPN no es una aplicación Web Proxy ni opera a través de un navegador Web, ya que opera sobre la capa 2 o 3 de la pila OSI. Por tanto, un cliente de OpenVPN no podrá utilizar un navegador Web para conectarse al servidor de OpenVPN y mantener una comunicación segura a través de la VPN.

OpenVPN es una herramienta multiplataforma soportada en sistemas operativos como Linux, Windows 2000/XP y Vista, OpenBSD, FreeBSD, NetBSD, Mac OS X y Solaris. Además, soporta autenticación del cliente mediante dos factores, permite utilizar políticas de acceso a usuarios y grupos específicos y reglas de firewall aplicadas a las interfaces virtuales utilizadas por OpenVPN para el filtrado de paquetes IP.

2.1.5. Otro software VPN

Además de las dos soluciones que hemos enfrentado para la realización del proyecto, hemos barajado más opciones. Aquí se detalla una pequeña lista con algunas opciones para crear una conexión VPN. Normalmente las opciones gratuitas imponen restricciones de velocidad, ancho de banda diario y/o limitan el número de servidores VPN a los que puedes acceder. Esto no sucede con las versiones de pago que proporcionan potencia y posibilidad de elección de los servidores, así como incluir algún servidor en algún punto geográfico concreto.

2.1.5.1. Free VPN

Desarrollado por WCS, es una de las mejores opciones que encontramos. Combina seguridad y velocidad, algo que generalmente no va de la mano. La latencia con la que se maneja esta entre 10 y 50 ms, una genialidad en relación con otras opciones. Es muy sencillo de instalar y de manejar.

2.1.5.2. It´s hidden

Es parte de Prot 80 Limited (Seychelles), una empresa holandesa reconocida por proporcionar VPN gratuito, así como también servicios de pago de VPN. En esta VPN se crea una conexión segura para cifrar todos los datos con 128 bits que protegen tu privacidad y te aseguran ante detecciones profundas. No se necesita instalar ningún software. Es multiplataforma y no guarda log de su actividad.

2.1.5.3. TorVPN

TOR es la respuesta al anonimato a través del navegador, siempre y cuando tu ISP lo permita manteniendo conducta ante la información de datos personales a las agencias que lo demanden. TOR VPN servirá especialmente para saltarse filtros de contenido, proteger una comunicación VoIP, acceder a datos en un terminal remoto a través de diferentes accesos como SSH, PPTP, Proxy TOR y más. La limitación de este servicio es de 1GB y funciona en Windows, Mac, iPhone e iPad.

2.1.5.4. LogMein Hamachi

Es un nombre compuesto por dos grandes del software, pero a la vez es un gran servicio VPN de la gente que está detrás del servicio de gestión remota de aplicaciones llamada LogMeIn. Es gratuito para uso no comercial y personal y no requiere hardware especial. Ofrece comunicaciones seguras, securización por túnel a través de redes públicas y privadas, una red flexible y combina la facilidad de uso de una SSL VPN con la conectividad de una VPN I. La gestión se basa en la web y es gratuita.

2.1.5.5. Cryptocloud

Servicio de pago, es uno de los proveedores de servicios VPN de alta calidad. Aun así, lo añadimos porque ofrece una prueba gratuita de 7 días, para los que quieren un acceso fortuito y potente. Te permite tener 2 cuentas VPN a las que puedes acceder simultáneamente para obtener la máxima seguridad posible, entrecruzando datos. Además posee un servicio de soporte sobre la marcha. Compatible con diferentes sistemas operativos y dispositivos móviles.

2.1.6. Softether VPN vs Open VPN

Partiendo de la base de que Open VPN es una magnifica herramienta, podemos observar que desde que se lanzó, hace ya algunos años (2002), no ha tenido actualizaciones significativas.

En la figura 7 se describe las características que posee SoftEther VPN respecto a OpenVPN. SoftEther VPN soporta protocolos VPN multiplataforma y usos de VPN nativos de múltiples sistemas operativos. SoftEther VPN posee una interfaz gráfica fácil e intuitiva. Se incluye soporte en varios idiomas. Además SoftEther VPN tiene la opción OpenVPN-Clone, esto significa que los usuarios de OpenVPN pueden migrar fácilmente a SoftEther VPN.

A continuación se adjuntan dos tablas de estudios de velocidad, realizados por empresas independientes. En ellos queda demostrado que la velocidad de SoftEther es mayor, en cualquier condición respecto a OpenVPN. Las unidades se expresan en Mbps.

Estudio realizado por HideIPVPN:

	OpenVPN	SoftEther
Velocidad de bajada	7.61	60.04
Velocidad de subida	9.05	86.64

Estudio realizado por VPNxD:

	OpenVPN	SoftEther
Velocidad de bajada	2.94	28.60
Velocidad de subida	4.94	4.32
Ping	108	120

OpenVPN vs. SoftEther VPN

	OpenVPN	SoftEther VPN
Initial Release	2002	2013
License	GNU GPL	GNU GPL
Developed by	OpenVPN Technologies, Inc.	SoftEther VPN Project, University of Tsukuba, Japan.
Source Code	C 91,000 lines	C / C++ 378,000 lines
Supported VPN Protocols	· OpenVPN only	· OpenVPN · L2TP/IPsec · L2TPv3/IPsec · EtherIP · Microsoft SSTP · VPN over HTTPS (SSL-VPN) · VPN over DNS · VPN over ICMP
Supported Native Built-in VPN Clients of Operating Systems	No	· Windows (L2TP, SSTP) · Mac OS X (L2TP) · iOS (L2TP) · Android (L2TP)
Throughput	< 100Mbps	> 900Mbps
NAT Traversal Function (UDP Hole Punching)	No	Yes
Dynamic DNS Function	No	Yes
VPN via HTTP Proxy	Yes	Yes
IPv6	Yes	Yes
Packet Filtering	No	Yes
Multi-Tenants Support	No	Yes
Delay, Jitter and Packet Loss Generator (Simulation Function)	No	Yes
Virtual DHCP & NAT Function	No	Yes
Listen on Multiple TCP/UDP Ports	No	Yes
Security Layer	OpenSSL	OpenSSL
Smartcards & USB Tokens	PKCS#11	PKCS#11
GUI Management	No	Yes (VPN Server GUI Manager)
CUI Management	Limited	Yes (Dynamic Configuration like Cisco IOS)
RPC over HTTPS Management	No	Yes
Config File Hand Writing	Yes	Yes
Multi-Language on UI	English only	English, Japanese, Chinese
Platforms	· Windows · Linux · FreeBSD · Solaris · Mac OS X · iOS · Android · NetBSD · QNX	· Windows · Linux · FreeBSD · Solaris · Mac OS X · iOS · Android

Figura 7 Comparativa OpenVPN vs SoftEther VPN

2.2. Secure Shell (SSH)

Desde que Internet ha comenzado a ser barato y disponible, ha empezado a derribar los antiguos métodos de comunicación como puedan ser el teléfono o el fax, además de ser la principal plataforma para llevar a cabo los accesos a las computadoras en las compañías.

Uno de los principales retos para reemplazar el sistema tradicional, es la seguridad. En el pasado, las compañías tenían sus propios bancos de módems para el acceso a los datos de la empresa. Esta tecnología era cara de mantener y sobre todo era muy poco escalable. En grandes compañías, con necesidad de numerosos accesos, esta solución era demasiado cara.

Secure Shell es un protocolo que provee de autentificación, encriptación e integridad de los datos para aumentar la seguridad a las redes de comunicaciones. Las aplicaciones SSH ofertan las siguientes capacidades: una consola de comandos segura, una transmisión segura de archivos y un acceso remoto a una gran variedad de aplicaciones TCP/IP a través de un túnel seguro. El cliente y el servidor Secure Shell está disponible en la mayoría de los sistemas operativos más comunes.

2.2.1. Funcionalidad de SSH

SSH se basa en tres pilares fundamentales, los cuales abren la puerta al diseño de variadas soluciones de seguridad.

2.2.1.1. Consola de comandos segura

Disponible en todos los sistemas operativos, proporciona la posibilidad de ejecutar programas u otros comandos, normalmente con la idea de ser impresos por pantalla. La consola de comandos segura permite editar, ver el contenido de directorios y acceder a aplicaciones de bases de datos. Los administradores de redes y sistemas pueden dar la orden de comenzar un trabajo remotamente, ver o parar procesos o servicios, crear cuentas de usuario, cambiar permisos a ficheros o directorios y muchas cosas más. Todo lo que puedes hacer en una máquina que tienes al alcance de tu mano, lo puedes hacer de forma totalmente segura en un ordenador remoto desde la carretera o tu casa.

2.2.1.2. Redirección de puertos

Es una herramienta muy potente que puede ofrecer seguridad a aplicaciones TCP/IP, incluyendo el correo electrónico, bases de datos de clientes y vendedores, y aplicaciones in-house. La redirección de puertos, algunas veces llamada túnel, permite que las aplicaciones TCP/IP, normalmente vulnerables, pasen a ser aplicaciones

seguras. Tras la activación del redireccionado de puertos, SSH redirige el tráfico del programa cliente y envía los datos a través de un túnel, cuya información esta encriptada, al servidor. La mayoría de las aplicaciones pueden transmitir sus datos a través de un único canal multiplexado, eliminando la necesidad de abrir puertos adicionales y haciendo más vulnerable el firewall o router.

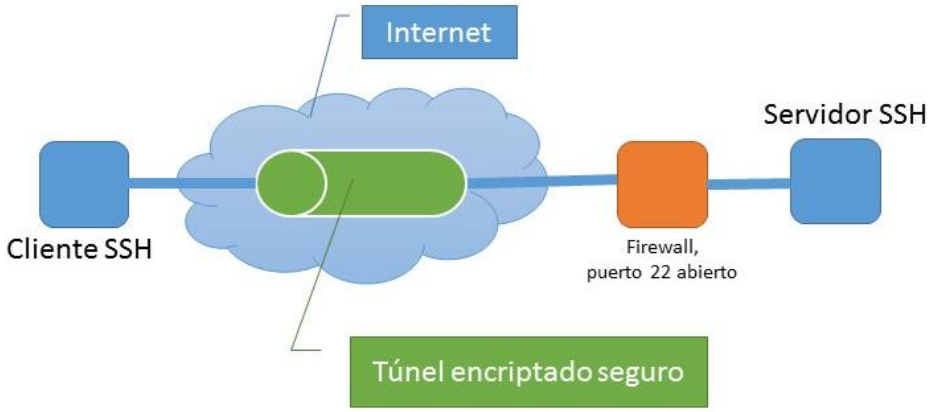

Figura 8 Túnel encriptado seguro

Para algunas aplicaciones, la consola de comandos segura no es suficiente y es necesario un acceso remoto a nivel gráfico. El redireccionamiento de los puertos de secure Shell puede ser usado para crear un túnel encriptado sobre la aplicación que está corriendo. Virtual Network Cliente (VNC), es un buen ejemplo.

2.2.1.3. Transferencia segura de archivos

El protocolo de transferencia segura de archivos (SFTP) es un subsistema del protocolo SSH. En esencia, es un protocolo para la trasferencia de archivos desarrollado sobre una capa del protocolo SSH. SFTP tiene múltiples ventajas sobre el inseguro FTP. Primero, SFTP encripta el usuario-contraseña y los datos que van a ser transferidos. Segundo, usa el mismo puerto que el servidor SSH, eliminando la necesidad de abrir otro puerto en el firewall o en el router. Usando SFTP te evitas los problemas relacionados con el NAT que tan comunes son con el protocolo FTP. Otro punto a tener en cuenta es la posibilidad de crear una extranet segura o fortificar un servidor o los servidores fuera de nuestro firewall.

Usando SFTP para crear una extranet segura para el compartición de archivos y documentos con clientes y socios teniendo en cuenta la necesidad de un acceso seguro a los datos. Los típicos usos son la creación de archivos, la compartición de estos, así como la creación de informes de la compañía o reportes de tareas pendientes.

Además, SFTP permite que estas transacciones sean automáticas sin intervención de ningún empleado.

La creación de una extranet segura es una de las maneras más seguras de compartir información específica con clientes, socios y empleados remotos sin poner en riesgo la información de la compañía en una red pública. Usando SFTP en tus máquinas de la extranet, estarás restringiendo el acceso a usuarios autorizados y encriptando los nombres de usuario, contraseñas y archivos enviados desde o a la DMZ

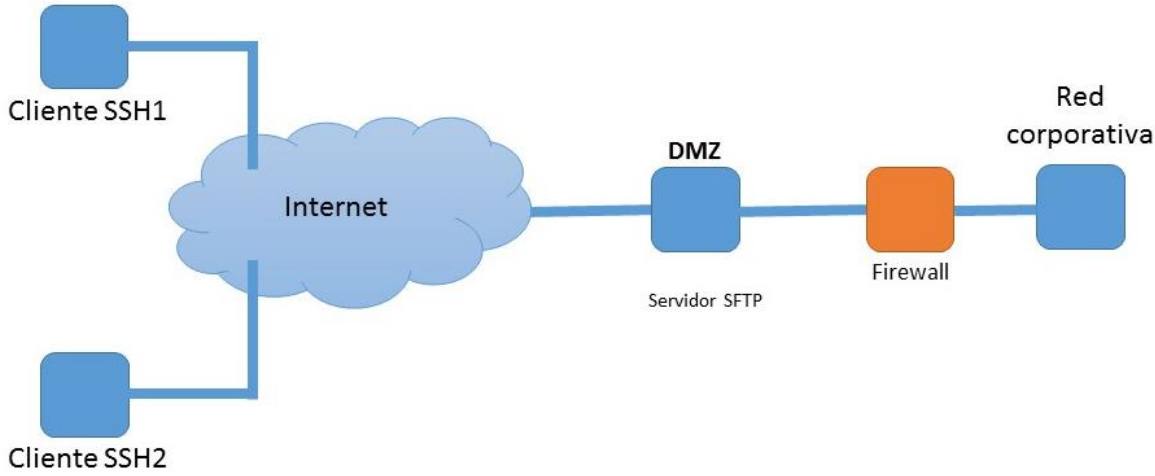

Figura 9 Accediendo a la red corporativa

2.2.2. Protocolos básicos del SSH

El protocolo SSH ofrece cuatro beneficios básicos de seguridad:

2.2.2.1. Autentificación de usuario

Significa que el sistema tiene que cerciorarse de que el usuario que está accediendo está permitido, y en caso contrario denegarle el acceso. Existen múltiples formas de autentificación, partiendo de los rangos específicos de contraseñas dependiendo de la familia del usuario a robustos sistemas de seguridad. La mayoría de implementaciones de SSH incluyen contraseña o utilización de una key, además de otros tipos de autentificación. Los protocolos de flexibilidad permiten que nuevos métodos de autentificación estén siendo añadidos constantemente.

Autentificación por password

Probablemente estemos ante el más más común de los métodos de autentificación. Al crear el usuario se le otorga una clave que será propia y en el momento de acceder tendrá que introducir estos dos parámetros, nombre de usuario y contraseña, si la combinación es correcta tendrá acceso a la información. Es un método que se queda corto y el cuál se recomienda combinar con otro tipo como puede ser el requisito de la key pública-privada.

Figura 10 Relaciones SSH

Autentificación por key.

Es uno de los métodos más seguros usados para autentificar dentro del protocolo SSH. La clave utiliza un par de claves generadas por ordenador, una pública y otra privada. Cada key suele estar entre los 1024 y 2048 bits de longitud y tiene un aspecto parecido al de la figura 11.

```
-----BEGIN RSA PRIVATE KEY-----
MIIEowIBAAKCAQEAj62POpNVW19j5xnqRpnmyQHbl
jz7t6biU5HFrKYmTVXNXAXRU+AE1hYpyTE4ugYos9
O+lR3iihLtIU11/5eER2Eh3ndApyLuaCUpsABWEgS
JKsIpLKdrfDmGguc4A76Ix7k9gc9mPdREbp5PJ/J+
dJ57HHDHcfgfvVu6x9DVqQdnPN/bexJ2/y9u4Dc4B
```

Figura 11 Contenido Private key

Suelen ser generadas usando una herramienta para la generación de claves. Tanto la key pública como la privada son creadas al mismo tiempo, están relacionadas y no son intercambiables. Algunas veces, las claves son utilizadas para acceder a un servidor que a su vez posee las claves para acceder a la información.

La clave privada nunca abandona el cliente, con lo que no puede ser robada como si de una contraseña se tratara. Normalmente la clave privada posee una “passphrase” asociada con ella, por tanto si es robada, el ladrón debería saber la frase con la que se relacionó a la key.

2.2.2.2. Autentificación del host

Una clave de host es usada por el servidor para probar que la identidad para el cliente y desde el cliente para verificar que es un host conocido.

2.2.2.3. Encriptación de los datos

Encriptación muchas veces se mezcla con privacidad, significa que tus datos están protegidos de algún ataque “sniffing”. Ciphers es el mecanismo por el cual SSH encripta y desencripta la información que es enviada. Los datos son manipulados con una key única, privada y compartida, y generalmente con múltiples rondas de manipulación con funciones no lineales. Los datos tras este punto están totalmente encriptados.

Cuando el cliente solicita la información, tras presentar los datos de acceso al servidor, este envía los datos encriptados al cliente, los recibe encriptados y el cliente es el encargado de deshacer el trabajo de encriptación que tan bien hizo el server.

2.2.2.4. Integridad de los datos

SSH garantiza que la información enviada desde un extremo ha llegado al otro extremo. Debido a que el encriptación en SSH, podía ser susceptible de introducir datos no deseados en el flujo de datos. La versión SSH 2 usa un código de autentificación del mensaje (MAC), lo que mejora el chequeo simple CRC de 32 bits de la versión inicial.

2.3. Cloud Computing

Según el NIST, National Institute of Standards and Technology, se define como el modelo para permitir el acceso conveniente, desde cualquier sitio y bajo demanda a la red con recursos informático compartidos y configurables, como por ejemplo: Servidores, Almacenamiento, Aplicaciones y Servicios. Que puede ser aprovisionado y liberado con un mínimo esfuerzo de administración o interacción con el proveedor.

Este modelo se compone de tres modelos de servicio y cuatro modelos de despliegue.

Figura 12 Cloud Computing

2.3.1. Características

La computación en la nube presenta características clave como las que se detallan a continuación.

2.3.1.1. Agilidad.

El usuario puede trabajar “en vivo” con su proveedor cloud, ante la necesidad de más capacidad de cómputo, tiene a golpe de un clic, la posibilidad de modificar su potencia, capacidad o cualquier otro ajuste.

2.3.1.2. Reducción de costes.

Quizá uno de los mejores puntos por los que el Cloud está en auge, dejando a un lado las máquinas propias en las empresas. Los proveedores aseguran el decremento del coste. Solo debemos pagar por la necesidad que tengamos, si necesitamos más servicios, nuestro proveedor nos lo ofrece, evitando una ampliación hipotética de los computadores propios debido a una actividad puntual.

2.3.1.3. Accesibilidad.

El acceso a estas plataformas, a día de hoy, es en cualquier lugar. Gracias a la conexión a internet podemos gestionar nuestras necesidades Cloud a través de dispositivos portátiles, oficinas o incluso móviles.

2.3.1.4. Elasticidad y escalabilidad.

Las aplicaciones en la nube son totalmente elásticas en cuanto a su sencillez de implementación y adaptabilidad. Además, son totalmente escalables. Ante la necesidad puntual de más capacidad, el servicio Cloud te provee de la potencia necesaria, de manera transparente al usuario.

2.3.1.5. Estabilidad.

Toda empresa necesita que su sistema sea estable, ante el fallo de cualquier máquina, el servicio no debería darse cuenta de ello. Los proveedores Cloud ofrecen máquinas activas y con posibilidad de servicio en todo momento, por tanto ante la posibilidad de

un fallo en cualquier computador, otra máquina tomará las funciones, y el usuario o empresa no se percatará de ningún problema.

2.3.1.6. Seguridad.

Es la principal inversión de los proveedores Cloud, quizá el punto de mayor controversia de estos servicios. La seguridad es tan buena o mejor que en los sistemas tradicionales, quizá debido a la centralización de los datos. La cantidad de recursos dedicados por los proveedores a este fin es enorme.

2.3.2. ¿Cómo funcionan?

2.3.3. Tipos de Cloud

2.3.3.1. Nube Pública

Es una nube computacional mantenida y gestionada por terceras personas no vinculadas con la organización. Los datos y los procesos de varios clientes son ejecutados en el mismo servidor, sistemas de almacenamiento u otras infraestructuras. Los usuarios no saben que trabajo corre en las maquinas del suyo propio. Aplicaciones, almacenamiento y otros recursos están disponibles al público a través del proveedor de servicios. El acceso remoto, solo se ofrece a través de internet.

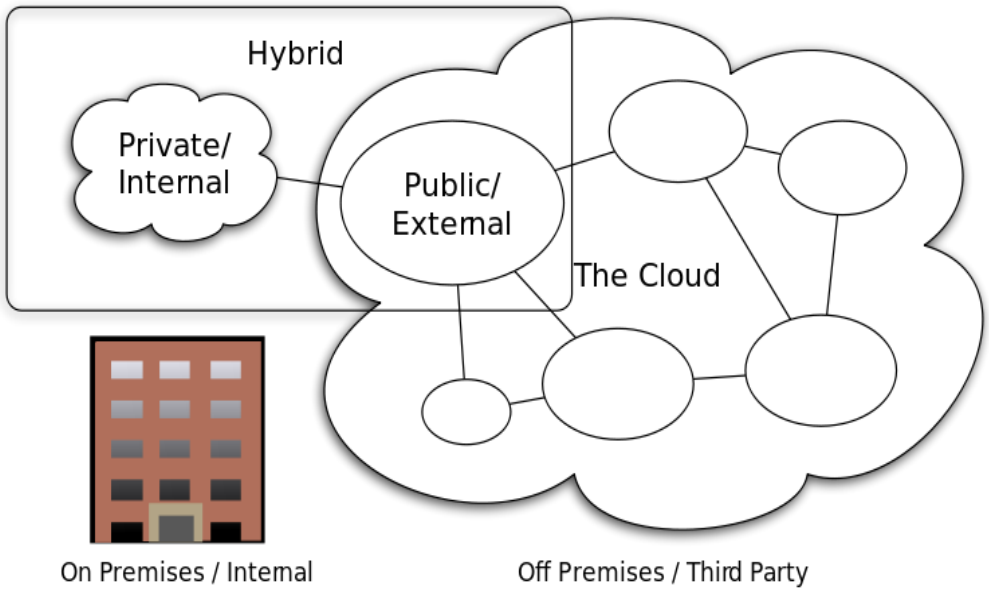

Figura 13 Tipos de Nube

2.3.3.2. Nube Privada

Son la opción a las compañías que desean un nivel de protección de datos alta. Las nubes privadas suelen ser bajo demanda, gestionadas por un solo cliente que controla qué aplicaciones debe ejecutarse y dónde. Son propietarios del servidor, red y disco y pueden decidir qué usuarios están autorizados a utilizar la infraestructura.

2.3.3.3. Nube Hibrida

Combinan modelos de nube pública y privada. Eres propietario de una parte y compartes otras, aunque de manera controlada. Se ofrece la promesa del escalado, pero siempre y cuando las aplicaciones no sean muy complejas y/o necesiten bases de datos complejas.

2.3.3.4. Nube Comunitaria

Más que un tipo, es una especificación del uso. La nube comunitaria, es aquella que es utilizada con un fin o función común. Pueden ser administradas por las organizaciones constituyentes o por terceros.

2.3.4. Modelos de Servicio

Cuando hablamos de Cloud Computing debemos tener en cuenta que podemos elegir entre tres modelos de servicio- SaaS, PaaS o IaaS- y que cada uno de ellos representa una estrategia distinta a la hora de la gestión.

2.3.4.1. Software como servicio

En inglés SaaS, “software as a service”, se encuentra en la capa más alta de los servicios Cloud. Se caracteriza por ofrecer una aplicación como un servicio por demanda y vía multitenencia, es decir, que una sola instancia del programa sirve para todas los clientes.

Las aplicaciones de este tipo, son accesible a través de un navegador o de cualquier aplicación diseñada a tal efecto. El usuario no suele tener total control sobre ellas, se le permiten pequeños cambios en las configuraciones. Esto permite liberar al cliente de

la necesidad de instalación de la aplicación en sus propios computadores, evitando los costes de soporte y el mantenimiento.

2.3.4.2. Plataforma como servicio

En inglés PaaS, “platform as a service”, es la oferta de plataformas computacionales, normalmente sistema operativo, entornos de desarrollo y APIs para lenguajes de programación, bases de datos y servidores web. El acceso se suele mover entre acceso web o acceso mediante SSH.

2.3.4.3. Infraestructura como servicio

En inglés, “infraestructura as a service”, renombrado por algunos como Haas, “Hardware as a service” se encuentra en la capa inferior y es un medio de entregar almacenamiento básico y capacidades de computo como servicios estandarizados en la red.

Abarca desde servidores, sistemas de almacenamiento, conexiones, enrutadores y otros sistemas para manejar cargas de trabajo, durante etapas de carga pico.

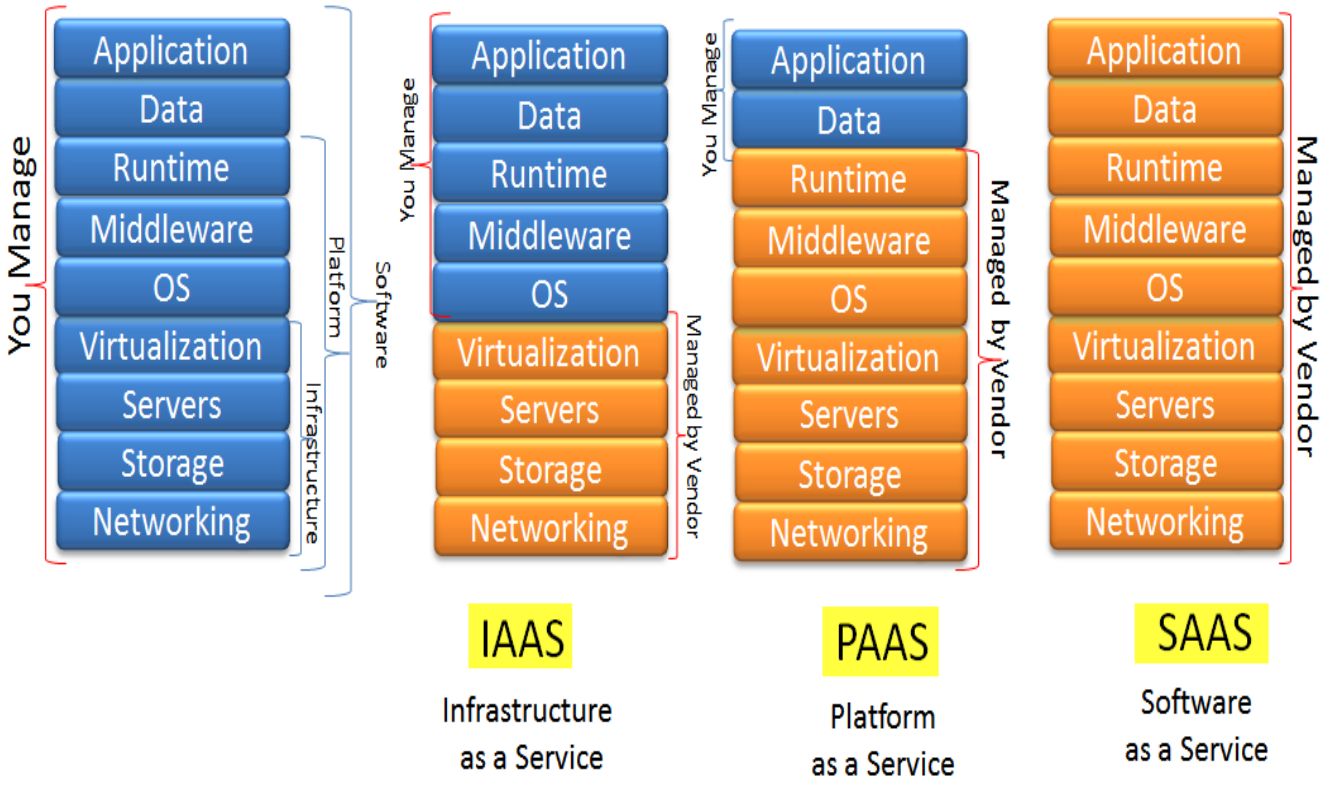

Figura 14 IaaS, PaaS y SaaS

2.3.5. Amazon Web Services

Amazon Elastic Compute Cloud es un servicio Web que proporciona capacidad informática con tamaño modificable en la nube. Según Amazon, se ha diseñado con el fin de que la computación web resulte más sencilla a los desarrolladores. Lo interesante de Amazon es su facilidad de escalar de forma horizontal. Agregando más procesador, más memoria, más almacenamiento, o más instancias, que vendrían a ser como más servidores trabajando en paralelo. Provee herramientas de recuperación de datos y aislamiento frente a otros procesos realizados en sus máquinas. En este tipo de servicio solo se paga por la capacidad utilizada. Se apoya en las tecnologías de virtualización, lo cual permite utilizar diversos sistemas operativos a través de sus interfaces de servicios Web.

2.3.6. Microsoft Azure

Es una plataforma que se ofrece como servicio y alojada en los centros de procesamiento de datos de Microsoft. Ofrece distintos servicios para aplicaciones, desde los que permiten guardar aplicaciones en alguno de los centros de procesamiento de datos de la compañía para que se ejecute sobre su infraestructura en la nube hasta otros de comunicación segura y asociación entre aplicaciones.

2.4. Sistemas de información geográfica

Los Sistemas de Información Geográfica (SIG o GIS, Geographic Information System en Inglés) son el resultado de la aplicación de hardware, software y procedimientos elaborados a datos geográficos para facilitar su obtención, gestión, manipulación, análisis, almacenamiento y representación con el fin de resolver problemas complejos de planificación y gestión.

2.4.1. ¿Cómo funcionan?

Los SIG funcionan como una base de datos geográfica que se encuentra asociada a los objetos gráficos existentes en un mapa digital, y dan respuesta a las consultas interactivas de los usuarios analizando y relacionando diferentes tipos de información con una sola localización geográfica.

La razón fundamental para utilizar un SIG es la gestión de información espacial. El sistema permite separar la información en diferentes capas temáticas y las almacena independientemente. Estas capas se superponen unas a otras y se pueden combinar en una visualización de mapa común. Esto hace que la tarea de relacionar la información existente para la obtención de resultados sea más rápida y sencilla.

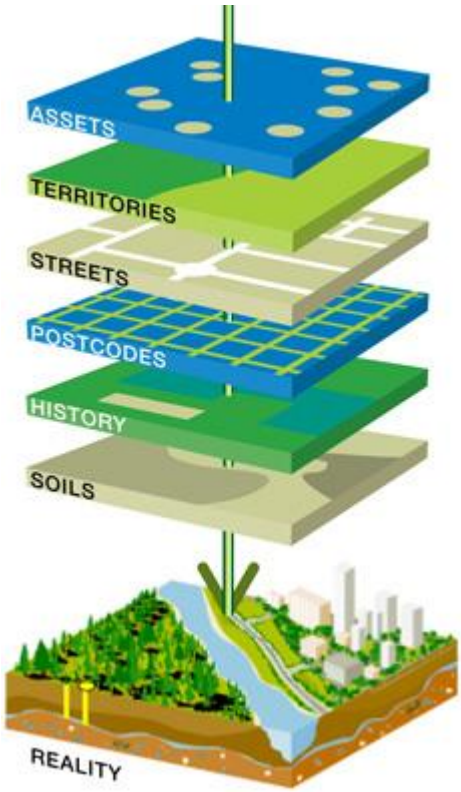

Figura 15 Capas de un SIG

2.4.2. ArcGIS

ArcGIS es un Sistema de Información Geográfica (SIG) que permite recopilar, organizar, administrar, analizar, compartir y distribuir información geográfica. ArcGIS permite publicar la información geográfica para que esté al alcance de cualquier usuario, desde cualquier lugar y desde diversas plataformas. Este sistema incluye software, una infraestructura on-line basada en la nube, recursos configurables y mapas base listos para usar, y contenido autorizado creado y compartido por la comunidad de usuarios SIG.

Una de las características de ArcGIS es que permite crear una amplia variedad de mapas, que no solo sirven para mostrar información, sino también como herramienta para

realizar análisis y modelado con el fin de resolver problemas específicos, permitir la entrada, la compilación y la síntesis de datos. Para realizar todo esto, ArcGIS cuenta con su propio conjunto de mapas base de diversos tipos, pudiendo el usuario crear sus propios mapas base.

Otra de las características de ArcGIS es que permite sintetizar datos de diversas fuentes en una misma vista geográfica unificada. Cualquier registro de información con una referencia geográfica puede localizarse y estar disponible en un mapa. También permite crear datos geográficos mediante digitalización inteligente, con la que es posible dibujar directamente en un mapa y almacenarlas en la base de datos geográfica del sistema.

ArcGIS también permite diseñar, crear, mantener y utilizar las bases de datos geográficas. Una base de datos geográfica hace posible que la información geográfica se almacene en un formato estructurado que simplifica la administración, la actualización, la reutilización y el uso compartido de los datos.

Admite también bases de datos multiusuarios de gran tamaño, por lo que esto facilita la administración y la actualización de los datos en grupos de trabajo de gran tamaño. Estas bases multiusuarios se implementan y facilitan en sistemas de bases de datos como Oracle, SQL Server, PostgreSQL, Informix y DB2.

Uno de los aspectos más interesantes y destacables de SIG es el análisis espacial. El objetivo que persigue es extraer nueva información de los datos existentes para permitir una mejor toma de decisiones.

Aunque asignar símbolos a los datos y visualizarlos en un mapa ya es una forma de análisis, el análisis espacial aplica operaciones geográficas, estadísticas y matemáticas a los datos representados en el mapa para poder resolver una amplia variedad de problemas distintos.

ArcGIS permite crear aplicaciones basadas en mapas. Este tipo de aplicaciones las emplean todo tipo de usuarios, por lo que pueden ser de propósito general como para tareas o actividades especializadas. Esta característica de ArcGIS es clave ya que no es preciso ser desarrollador para poder crear aplicaciones.

Por último, poder dar a conocer y compartir información es la parte más gratificantes de SIG. El sistema ArcGIS facilita la labor de comunicar y compartir el trabajo y de brindar eficaces mapas, visualizaciones y funcionalidades a otras personas sin necesidad de que sean expertos en SIG.

2.5. Java

Java es un lenguaje de programación con el cual podemos realizar cualquier tipo de programa. Durante la carrera, quizá ha sido el lenguaje de programación más utilizado.

En la actualidad es un lenguaje muy extendido y que cada vez está cobrando más importancia en el ámbito de internet y la informática en general. Está desarrollado por Sun Microsystems.

Una de las principales características de Java es la independencia de la plataforma. Eso quiere decir que podemos realizar un programa en Java que pueda funcionar en cualquier ordenador o dispositivo. Esto se consigue gracias a una máquina de Java que se ha creado para ser puente entre el sistema operativo y el programa compilado de Java, el *ByteCode* y posibilita que se entienda perfectamente.

2.5.1. Librerías y API´s

2.5.1.1. JSCH

Librería que simula el comportamiento de SSH2. JSch permite conectar a un servidor SSH y usar redireccionamiento de puertos, redireccionamiento X11, trasferencia de archivos y puedes integrarla fácilmente en tus programas en Java. JSch está desarrollado bajo licencia BSD.

Originalmente, la librería fue desarrollada con la idea de ofrecer WIredX, disfrutando de las sesiones X seguras. La posibilidad del redireccionamiento de puertos, dio pie a la realización y modificación de esta implementación.

Por ultimo aclarar, que esta librería refleja el comportamiento de SSH2, debido a la caducidad de la patente RSA de SSH1 y algunos arreglos en la integridad de los datos que se hicieron partiendo de la primera versión

2.5.1.2. ArcGis

El SDK de ArcGIS para Java provee un conjunto de herramientas de desarrollo que permiten crear aplicaciones con mapas 2D para ser utilizadas en Windows y en Linux. El SDK (Software Development Kit) permite integrar mapas tanto online y como locales, y modelos de geoprocesamiento para crear aplicaciones SIG altamente funcionales.

En un escenario con conexión a Internet, la aplicación puede obtener contenido y servicios de ArcGIS Server y ArcGIS Online. En un escenario desconectado(los usuarios no disponen de conexión a Internet) se puede dotar a los dispositivos con paquetes

locales que contienen mapas de los archivos GIS, datos y herramientas de geoprocesamiento con las que el usuario puede trabajar mientras esta desconectado.

El SDK permite una utilización modular, puedes seleccionar el subconjunto de componentes de ArcGIS Runtime necesario para dar soporte a la funcionalidad GIS que has elegido incluir en tu aplicación.

2.6. Web Service

Un servicio web es una tecnología que utiliza un conjunto de estándares y protocolos utilizados para intercambiar datos entre aplicaciones. Aplicaciones totalmente distintas y ejecutadas sobre cualquier plataforma, puede intercambiar datos en redes de ordenadores utilizando los servicios web.

La interoperabilidad se da gracias a la adopción de estándares abiertos. Existen dos organizaciones, OASIS y W3C que son las encargadas de la reglamentación de estos servicios.

En definitiva es una máquina que atiende las peticiones de los clientes web y les envía los recursos que estos solicitan

Respecto al formato estándar para los datos que se intercambian en un servicio web, XML es adoptado por todos ellos. Por ejemplo en nuestro caso, el servicio web nos devuelve el posicionamiento e información de las máquinas con las que trabajamos.

En la siguiente imagen podemos ver el comportamiento de un servicio web:

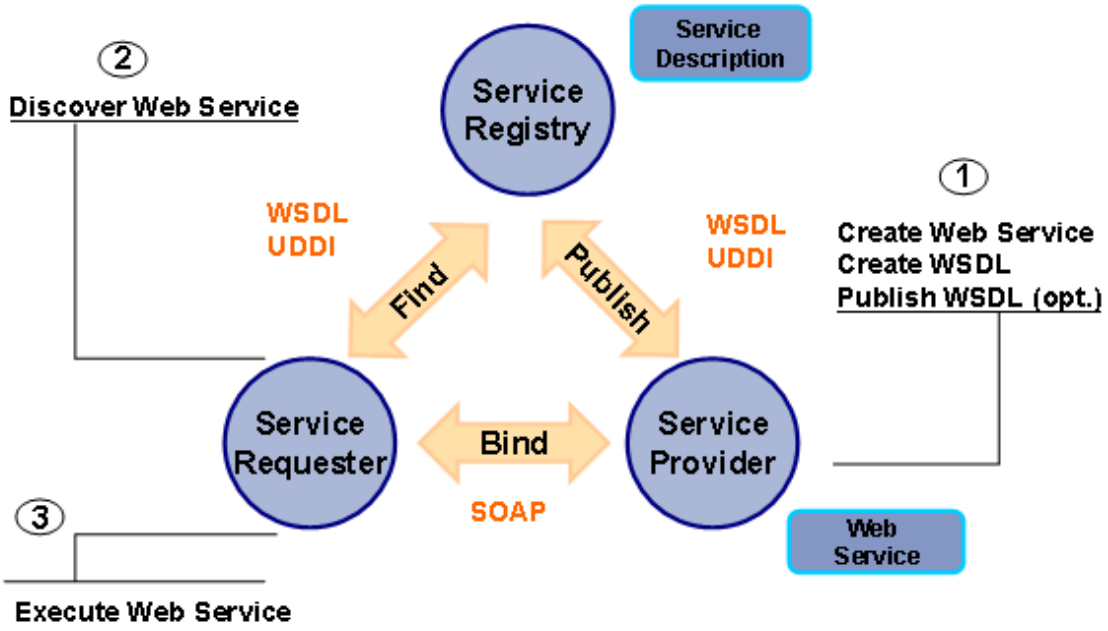

Figura 16 Esquema de funcionamiento Servicio Web

3. Arquitectura del sistema

3.1. Aproximación de alto nivel

Para resumir el formato y la arquitectura de Personal AnonyCloud lo dividiremos en distintos bloques:

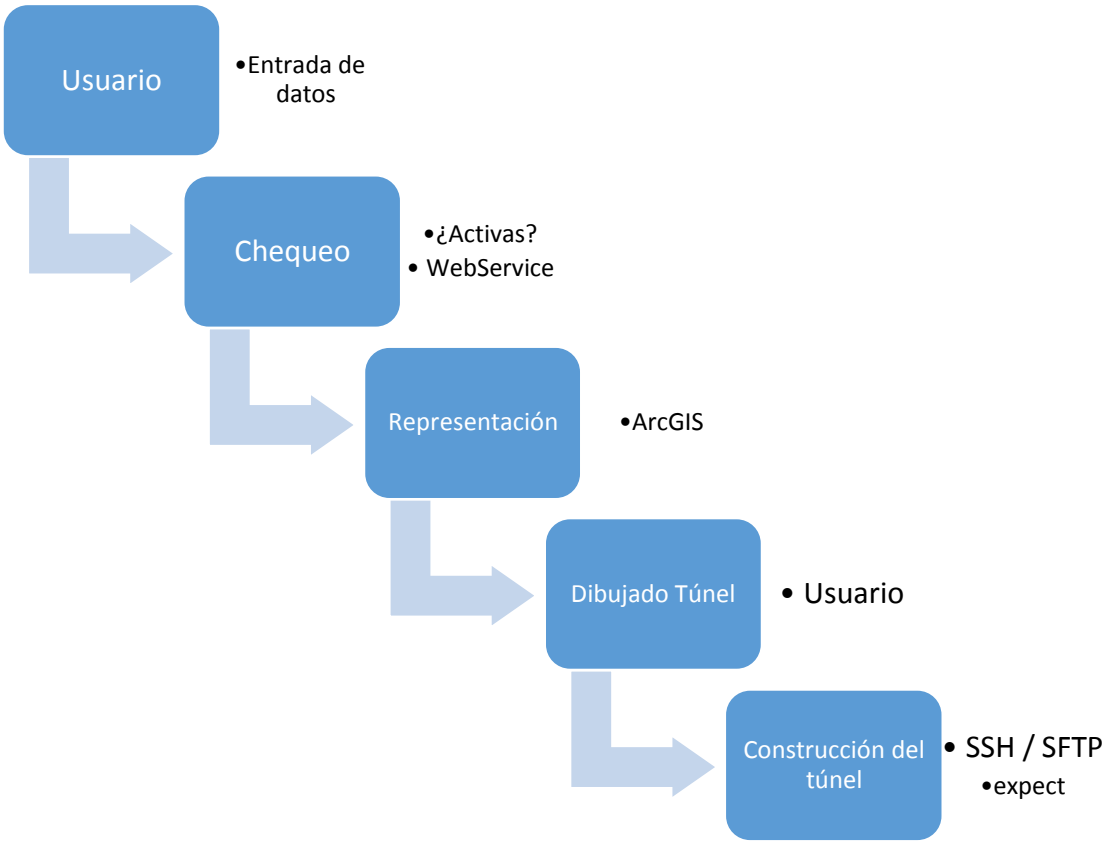

Figura 17 Arquitectura Personal AnonyCloud

- **Datos de entrada**, aportados por el usuario. El usuario deberá añadir a la aplicación las claves privadas para sus máquinas, así como un listado de estas.

- **Chequeo**, en este bloque se realizan dos consultas, la primera para saber si las máquinas están disponibles para su uso. Esta comprobación se realiza a través del comando isRecheable, que actúa como un ping por ICMP. La otra consulta es la situación geográfica de la IP publica de la máquina, esta se realiza a través de un servicio web que nos devuelve las coordenadas y la información de la máquina, en caso de fallo de conexión con dicho servicio web, hemos diseñado una cache de IP´s, que nos facilitará la información necesaria para que nuestro software funcione independientemente del servicio web.

- **Representación** en el mapa de las máquinas. Gracias a la plataforma ArcGIS las máquinas se ven representadas en el mapa, con la comprobación de disponibilidad ya realizada.

- **Dibujado** o borrado del túnel por parte del usuario. El usuario a través de simples clics y guiándose por los botones del menú.

- **Creación del túnel.** Digamos que la fase más difícil de entender para un usuario medio, por tanto es la parte de automatización. Se utiliza SFTP para la subida de los archivos a las máquinas remotas y se produce la ejecución del software en ellas.

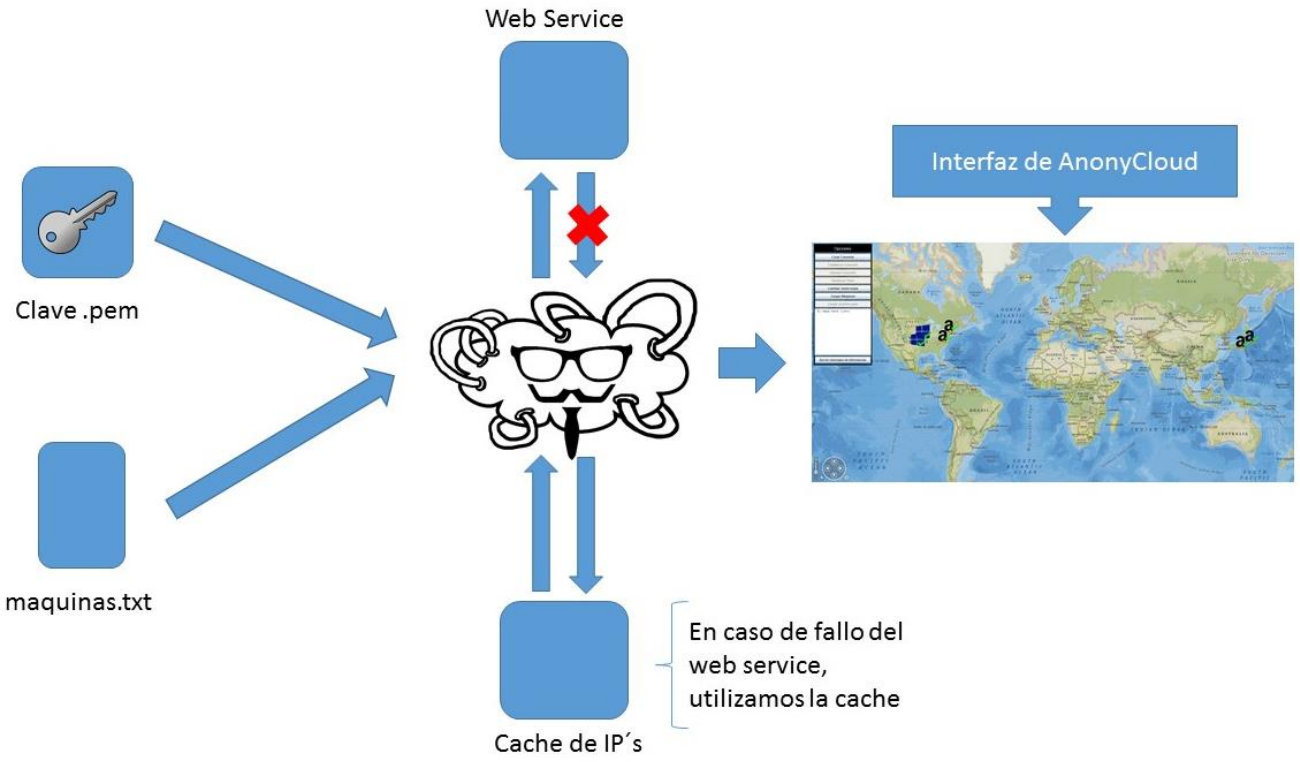

Figura 18 PA en sus tres primeras fases

3.1.1. Entrada de datos

La aplicación procesara dos tipos de ficheros, los archivos de clave privada .pem correspondientes a las máquinas y el archivo de máquinas del usuario.

Las claves serán en formato .pem, el sistema se cerciorará de que existen las claves necesarias para que la construcción del sistema sea posible y correcta.

Para las máquinas de usuario, de igual modo, se añadirán a través de un botón en el menú y el usuario añadirá un solo archivo con las máquinas, en el formato indicado en el apartado 3.3.2.1.

Una vez añadidos estos dos elementos el sistema procede a procesar dichos datos.

3.1.2. Confirmación de disponibilidad

En esta parte el sistema recibe la información de las máquinas y traslada peticiones al servicio web para averiguar el posicionamiento de la máquina por la que se pregunta.

Antes de realizar la petición se ha comprobado que las máquinas son accesibles y están operativas.

Habiendo mandado la dirección IP, el servicio web responderá con un XML en el que se detalla la latitud y longitud. Además podemos recuperar datos como el país, la región o el código postal.

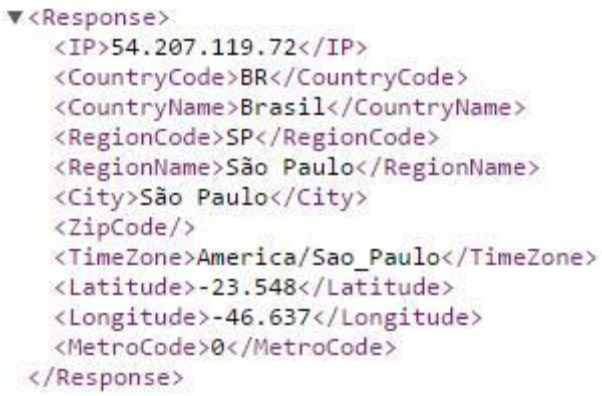

Figura 19 Formato XML servicio web

En caso de fallo de este sistema utilizaremos la cache IP. Este punto está detallado en decisiones de diseño, exactamente en 3.3.4.

Una vez que salimos de esta etapa sabemos cómo hay que dibujar las máquinas. Por tanto la siguiente fase será una fase de representación en el mapa con todos estos datos.

3.1.3. Representación en el mapa

El sistema representa en la interfaz la posición de las máquinas del usuario en el mapa. En esta fase la persona que este ejecutando PA puede ver la situación exacta de sus máquinas alrededor del mundo.

Se realiza sobre el trabajo de la plataforma ArcGIS, un servicio de información geográfica como se comentó en el punto 2.4.2. Los iconos de representación para cada máquina se detallan en el punto 5.3.

3.1.4. Manipulación del túnel

La parte interactiva, en la que el usuario decide crear y elegir las máquinas que serán la base para su túnel IP. La representación en ArcGIS promueve que el usuario interactúe con los botones del menú y a través de clics en el ratón puede conectar las diferentes máquinas. Tras la manipulación y elección del trazado perfecto del túnel, el usuario hará clic en realizar conexión (en el menú).

Esto hará que se lance la parte más Personal AnonyCloud.

3.1.5. Construcción de la estructura de túneles VPN

Ahora viene la parte interesante, el cliente empieza a interactuar con todas las máquinas que el usuario ha decidido que pertenezcan a su túnel.

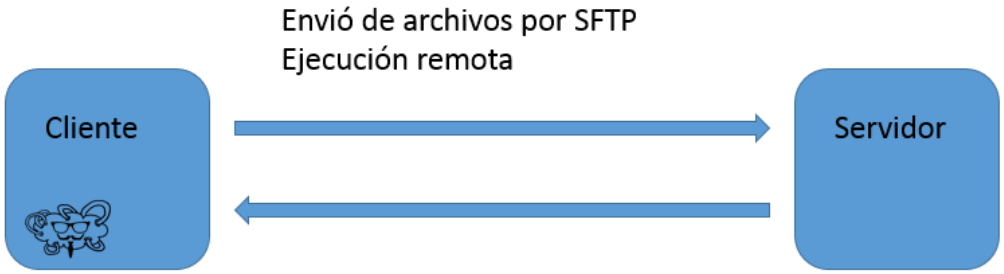

Figura 20 Intercambio Cliente-Servidor

La secuencia de instalación comienza por una conexión por SSH a nuestra máquina remota y el envío de un script en el que se detalla las instrucciones para la instalación automatizada de todo el software necesario.

```
#!/bin/bash



wget http://www.softether-download.com/files/softether/v4.15-9546-beta-2015.04.05-tree/Linux/SoftEther_VPN_Server/64bit_-_Intel_x64_or_AMD64/so
64bit.tar.gz


tar xzvf softether-vpnserver-v4.15-9546-beta-2015.04.05-linux-x64-64bit.tar.gz

cd vpnserver

expect <<- DONE

spawn sudo make

#Do you want to read the License Agreement for this software ?
#1.yes
#2.no

expect "*number:*"

send -- "1\r"

#Did you read and understand the License Agreement ?
#(If you #couldn't read above text, Please read'ReadMeFirst_License.txt'
#file with any text editor.)

expect "*number:*"

send -- "1\r"

#Did you agree the License Agreement ?
#1. Agree
#2. Do Not Agree

expect "*number:*"
```

Figura 21 Aspecto de script de instalación

Como peculiaridad el sistema debe modificar el estado del NAT en la última máquina para que se produzca el cambio de la IP.

3.2. Objetivos y restricciones

3.2.1. Objetivos

La motivación principal de Personal AnonyCloud es desarrollar una herramienta que permita el acceso a otro nivel de seguridad a usuarios que en un principio no poseen grandes conocimientos de redes. Esta herramienta tiene que ser:

3.2.1.1. Sencillo e intuitivo

Intentamos ocultar toda información que sea innecesaria, está diseñado por y para ser fácil de uso. Por ello se incluyen decisiones de diseño como por ejemplo, una interfaz con botones simples y entendibles, y una interfaz muy poco recargada.

3.2.1.2. Transparente al usuario

El usuario no debe de tener conocimiento alguno de redes y seguridad. El Software AnonyCloud instala en las máquinas el software necesario para que se lleve a cabo y se pueda construir el túnel VPN. La automatización de las instalaciones en todas las máquinas permite al usuario olvidarse de instalación en servidores y manipulación de tablas.

3.2.1.3. Vista Geográfica

Disponer de un mapa en el que situar y tener la posibilidad de una vista geográfica de todas las máquinas que posee el usuario. Este objetivo se fija tras estudiar otro software VPN. En ninguna aplicación podemos situar nuestras máquinas en un mapa y saber la posición exacta y poder intuir las diferencias de velocidad por proximidad.

3.2.2. Restricciones

3.2.2.1. Necesidad de conexión a Internet

Necesidad de conexión de banda ancha

3.2.2.2. El cliente solo está disponible para Sistemas Windows

Actualmente el cliente VPN de SoftEther, solo se encuentra disponible para el sistema Windows.

3.2.2.3. Sistema operativo en las máquinas virtuales

Es necesario que las máquinas virtuales funcionen sobre una imagen del sistema operativo Ubuntu, o bien del sistema operativo AMI Linux.

3.3. Decisiones de diseño

3.3.1. Eligiendo el Servicio Cloud

En primera instancia el proyecto se enfoca en el diseño y trato de las máquinas de Amazon Web Services. Debido a la facilidad y a la disponibilidad por parte del coordinador de este proyecto de ofrecernos dichas máquinas. Y también por la capa gratuita que ofrece AWS para usar sus máquinas en la nube, que es extrapolable para potenciales usuarios de la aplicación.

Más tarde se incluyen máquinas cuyo proveedor es Microsoft Azure.

Respecto a la diferencia entre ambas, las máquinas de Microsoft Azure ofrecen la autentificación con password. En cambio las máquinas de AWS, ofrecen la autentificación a través de una clave pem. Por cada región, AWS obliga a crear una clave pem distinta.

3.3.2. Carga de archivo de máquinas

El usuario facilitará la información de todas las máquinas que posee o quiera que formen parte de su enjambre en Personal Anonycloud. El usuario facilitará informaciones relativas a las maquinas como:

- Nombre de usuario de la máquina
- Nombre del host
- Nombre de la clave Pem o contraseña (caso de Azure)

3.3.2.1. Formato del archivo

El formato del archivo de texto que contiene las máquinas será el que se detalla en la figura 22.

```
1  # NombreUsuario   NombreHost   NombrePem/PassWord
2
3  ubuntu ec2-54-158-178-231.compute-1.amazonaws.com jl-anonycloud.pem
4  ubuntu ec2-54-159-174-181.compute-1.amazonaws.com jl-anonycloud.pem
5  azureuser albertovm1.cloudapp.net XX**PASS**XX
6  azureuser albertovm2.cloudapp.net XX**PASS**XX
```

Figura 22 Formato de maquinas.txt

3.3.3. Carga de claves .pem

El usuario deberá cargar los archivos .pem que posea para todas aquellas máquinas que haya añadido en el fichero de máquinas. Para evitar mal entendido con las rutas, y la disponibilidad de las rutas de las claves en un fichero que podría caer en malas manos, solo se incluye el nombre y se agregan a la aplicación de AnonyCloud.

Se carga a través de una ventana que se abre al hacer clic en el botón “Cargar archivo pem”

3.3.4. Cache IP

Debido al posible fallo del servicio web que nos facilita el posicionamiento de la máquina y por tanto la imposibilidad de representar en el mapa las máquinas, realizamos un cacheo de IP´s más utilizadas por el usuario. Guardamos la relación entre la dirección IP de una máquina y su geoposicionamiento, para la posterior utilización por ArcGIS

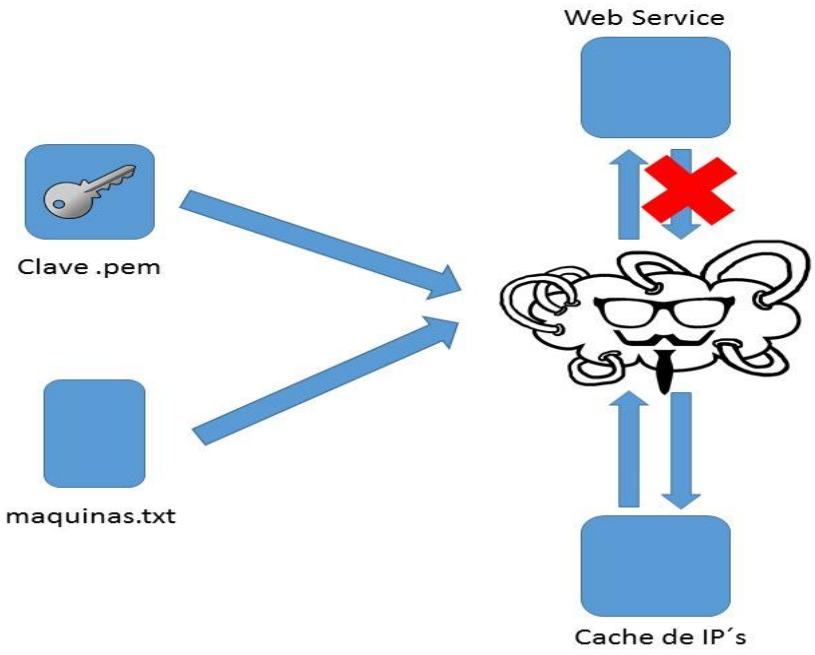

Figura 23 Esquema Cache IP

3.3.5. ArcGIS

Nos decidimos por el sistema ArcGIS por diferentes motivos:

- Acudimos a una sesión de presentación en la facultad y vimos que se ajustaba a los requisitos que necesitábamos para el proyecto.
- En el momento de trabajar con la herramienta, nos dimos cuenta de que ArcGIS facilitaba la representación y la manipulación de datos y/o elementos gráficos a través de una interfaz. Por tanto, era una solución idónea para el proyecto.

4. Conclusiones

4.1. Principales Conclusiones

Personal Anonycloud afronta problemas comunes hoy en día. Hemos puesto en práctica nuestros conocimientos para evaluar las propuestas de software similar, analizar el punto común que ninguno de ellos facilita. Hemos fijado nuestro objetivo y hemos realizado el proyecto.

Respecto al desarrollo del software, hemos aprendido acerca del Cloud Computing, de túneles VPN y de Security Shell. Además de tecnologías de representación geográfica.

Hemos aprendido a resolver problemas que pueden ser comunes en el desarrollo de proyectos de índole similar a este, hemos mejorado nuestros conocimientos y podemos decir que somos capaces de tomar decisiones con más seguridad en temas relacionados.

4.2. Conocimientos adquiridos

Detallamos los puntos más importantes, los pilares principales en los que se ha movido nuestro proyecto y por tanto aquellas áreas en las que hemos mejorado nuestras habilidades y conocimientos.

4.2.1. Computación en la nube

Gracias a la realización del proyecto, hemos adquirido conocimientos del funcionamiento del Cloud como Infraestructura como servicio, habiendo usado tanto Amazon Web Services o Microsoft Azure.

En un mundo en el que la tendencia hacia el Cloud es clara y tremendamente creciente, los conocimientos adquiridos nos permiten abrir nuevos campos de trabajo, o incluso ayudarnos en un hipotético uso de las infraestructuras desde una Startup o empresa fundada por nosotros.

Destacar la elasticidad, flexibilidad y la reducción del costo que ha repercutido en el proyecto.

4.2.2. Servicio VPN

Uno de los pilares principales del proyecto, hemos comprendido cómo funcionan los túneles VPN, la utilización de estos en todas las áreas en las que nos veremos involucrados en un futuro empleo.

El VPN es la forma más segura de interconectar dos elementos de manera segura, privada y con garantía de realizarse con éxito.

Hemos descubierto múltiples proveedores de servicios VPN, en esta memoria se han detallado algunos. Hemos aprendido las diferencias, las características de cada uno y hemos optado por SoftEther.

4.2.3. Secure Shell

El segundo pilar del proyecto, utilizado desde el primer momento para hacer pruebas en local, hemos aprendido como usar SSH para administrar, para transferir archivos de una máquina a otra o asegurar nuestros túneles VPN.

Conocimientos útiles para la administración de sistemas, supervisión y ejecución de trabajos en máquinas remotas o envío de archivos desde una terminal a otra.

4.2.4. Java como herramienta de desarrollo

Herramienta muy utilizado por todos nosotros en el transcurso de la carrera, La hemos situado en este área de conocimientos por la fluidez que hemos ganado en el tratamiento de librerías.

Hemos utilizado librerías que simulan comportamientos de una Secure Shell o las librerías de ArcGIS.

4.2.5. ArcGIS como medio de representación

Con la utilización de ArcGIS en nuestro proyecto hemos aprendido a usar una de las características más importantes de un SIG que es la representación por capas de la información, a localizar correctamente nuestros datos en el mapa para poder usarlos y modificarlos posteriormente en la interfaz.

También hemos aprendido a proyectar y representar puntos en distintas referencias espaciales, lo cual nos ha permitido ampliar el uso de distintos mapas en nuestra aplicación y poder representar todas las coordenadas en una misma referencia espacial.

4.2.6. Shell Scripting

Hemos ampliado nuestros conocimientos sobre shelll script con el uso y practica con el paquete expect. Este nos permite la interacción automática con máquinas remotas, dicho paquete permite quedarse a la espera de un patrón en la consola remota, de tal forma que se produzca respuesta automática, habiendo sido detallada la respuesta en el script.

4.3. Características y capacidades de Personal AnonyCloud

4.3.1. Funciones básicas

En Personal AnonyCloud, el usuario puede:

- Añadir sus máquinas al sistema: Amazon con distribuciones Ubuntu y Linux AMI y Azure.
- Añadir las claves propias de sus máquinas.
- Visualizar sus máquinas en un mapa.
- Dibujar la estructura que desee para un túnel VPN.
- Activar o desactivar máquinas.
- Borrar el túnel VPN dibujado.
- Armar o desarmar el túnel VPN.
- Cambiar el tipo de mapa en el que se visualizan sus máquinas.
- Seleccionar la máquina que hará de traductor NAT.

- Añadir un terminal más a un túnel existente.

Respecto al sistema, automáticamente realiza las siguientes funciones básicas:

- Obtener localización geográfica de las máquinas.
- Ejecutar scripts de manera remota.

4.4. Problemas encontrados durante el desarrollo

4.4.1. SoftEther VPN

No nos podemos referir al siguiente punto como el mayor problema resuelto, pero si la mayor dificultad o lo que más nos retrasó en el comienzo del desarrollo de Personal Anonycloud. Durante los primeros meses en los que barajamos distintas opciones para el software de creación del VPN, SoftEther nos produjo una gran carga de tiempo de estudio y entendimiento de todas sus configuraciones.

SoftEther posee configuraciones predefinidas, por ejemplo la conexión por VPN de un teléfono móvil a un ordenador, o el acceso simplemente de un ordenador a otro. Además de posibilidades cloud to cloud o LAN to LAN.

4.4.2. Automatización de scripts

El problema que nos encontramos en este punto era que no encontrábamos la manera de interactuar automáticamente con órdenes desde una terminal, una instalación del software en remoto. Tras varios intentos, decidimos probar con el comando *expect*, este comando actúa de tal forma que se encuentra esperando un patrón determinado en la consola y escribe automáticamente en consecuencia de lo leído.

Esto fue muy utilizado para la aceptación automática de permisos, así como la elección de las distintas funciones dentro de la consola del propio SoftEther.

4.4.3. Uso y manipulación de coordenadas

Al trabajar con las coordenadas en el sistema de ArcGIS, encontramos problemas al representar las máquinas en el plano, debido a que las coordenadas en las que se pintaban, no correspondían con la representación de las coordenadas del clic del ratón.

ArcGIS representaba las máquinas a través de la longitud y latitud de las máquinas. De tal forma que al realizar el evento del ratón, las coordenadas en las que se hacía clic se devolvían como coordenada (X,Y).

4.5. Trabajo futuro

Los siguientes puntos son fruto de una lluvia de ideas para mejorar y continuar el desarrollo de este boceto de PA.

4.5.1. Múltiples túneles

Esta línea de trabajo busca permitir que el usuario tenga configurados/dibujados diferentes túneles VPN, de tal forma que pueda elegir cuál usar en cada momento. Pudiendo decidir según las métricas de seguridad, velocidad o nivel de carga.

4.5.2. Combinación con VPN Azure Service

Como primer paso, queremos referirnos al punto 2.1.3.3. de la memoria, en el cuál se detalle los principales detalles de este servicio que ofrece SoftEther VPN.

Quitando la vista de uno de los pilares fundamentales del proyecto, y suponiendo la seguridad de un sistema público, VPN Azure Service nos proporciona una red bastante extensa de máquinas, situadas en el cloud de Microsoft, las cuales podremos usar pasar establecer nuestra conexión VPN de una manera más segura.

4.5.3. Realización para LANs

Al igual que hemos realizado el proyecto para configuraciones punto a punto, esta configuración permitirá utilizar desde cualquier de los ordenadores de tu red, el túnel VPN creado por una de sus máquinas hacia el exterior.

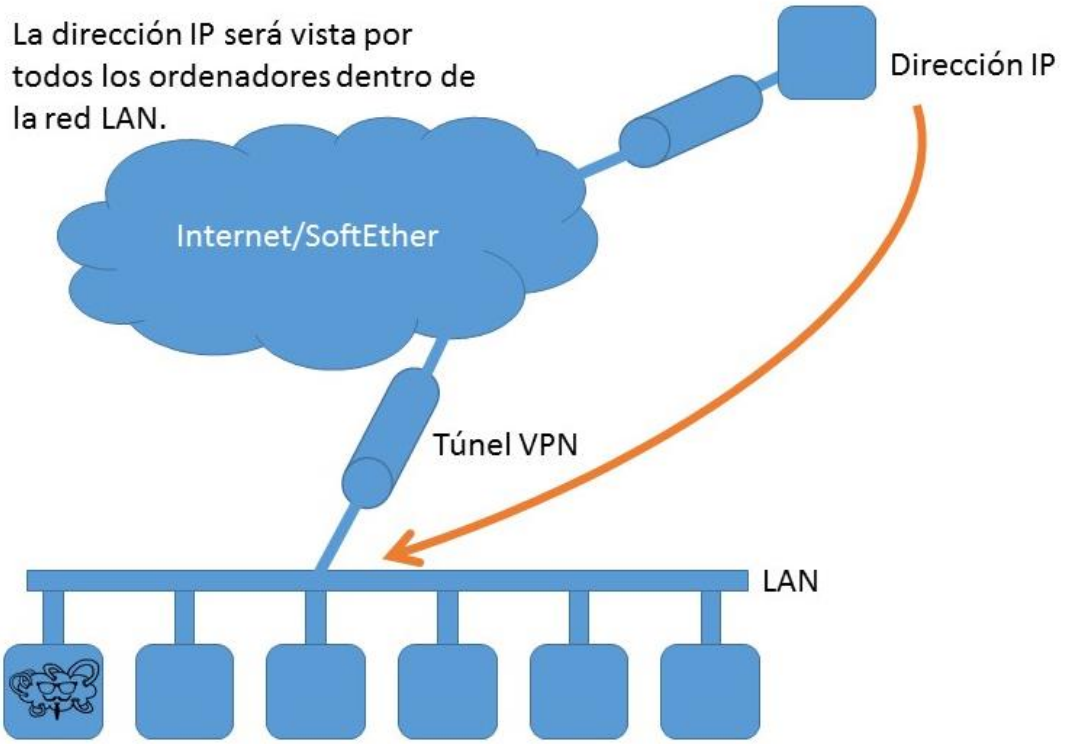

Figura 24 Esquema LAN to LAN

4.5.4. Gráfica de estudio de la seguridad de tu conexión.

Facilitar al usuario unas métricas precisas acerca de la seguridad y velocidad de los túneles creados. La idea es inventar un tipo de métrica que te permita facilitar la decisión de elección en una posible configuración con varios túneles VPN o simplemente informarte del nivel de seguridad que posees en el momento actual, con tu conexión VPN activa.

En la gráfica tendríamos en cuenta parámetros como:

- Cantidad de máquinas que tienen parte en el túnel creado.
- La distancia entre dichas máquinas.
- La velocidad de las conexiones y el posible retardo.
- Proveedor Cloud de máquinas.

4.5.5. Facilitar la conexión con máquinas pertenecientes al usuario

Añadir la posibilidad de que el usuario añada máquinas propias en la generación del túnel, de tal forma que pueda contratar máquinas fuera de los dominios de proveedores cloud como AWS o Azure y pueda utilizarlos de la misma manera.

4.5.6. Automatización de carga de máquinas desde servicios Cloud

En este punto existen dos posibilidades:

- La inclusión de los perfiles del usuario de los proveedores de servicios cloud. El usuario iniciaría con las credenciales de cada servicio cloud, y automáticamente las máquinas son incluidas en el mapa. Quizá esta idea sea la más elegante, pero ya comprometemos contraseñas y nombres de usuario, además de tener que tratar directamente con las APIs de los servicios Cloud.

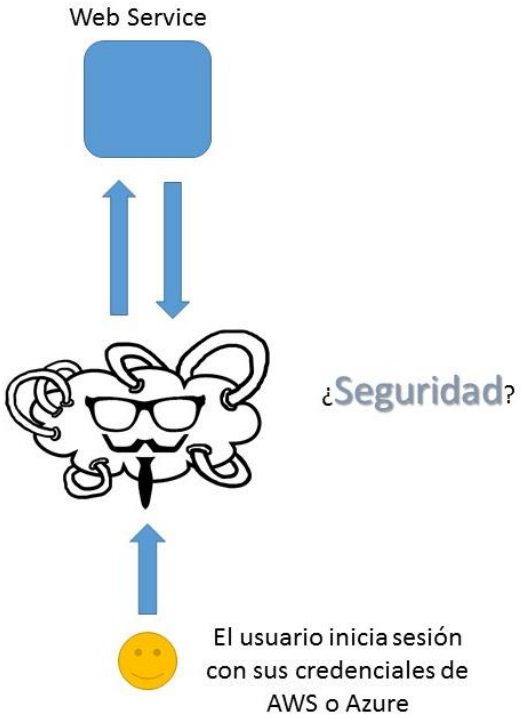

Figura 25 API cloud + PA

- Por momentos puede parecer el primer punto, pero difiere en la forma de tratar los datos. Tras la autentificación del usuario en los servicios cloud, esta aplicación obtendría los datos de las máquinas y crearía un archivo de máquinas cifrado.

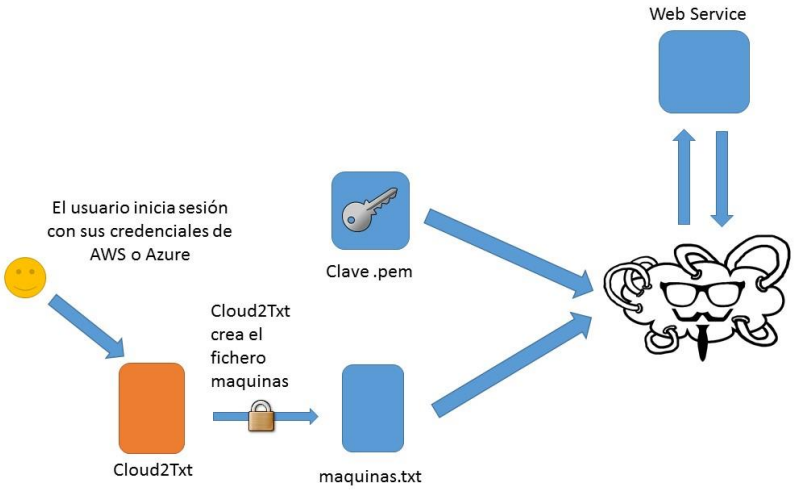

Figura 26 API creando maquinas.txt

De tal forma que la forma de uso de Personal AnonyCloud no se vería modificada, y el usuario vería facilitado su trabajo, solo incluyendo nombre y contraseña de los servicios cloud, y el archivo maquinas.txt se generaría automáticamente e incluyendo un cifrado.

4.5.7. Cliente Linux

Desarrollar PA para clientes Linux de manera automática, lo que nos permitiría usar PA de forma totalmente trasparente al usuario en entornos Ubuntu.

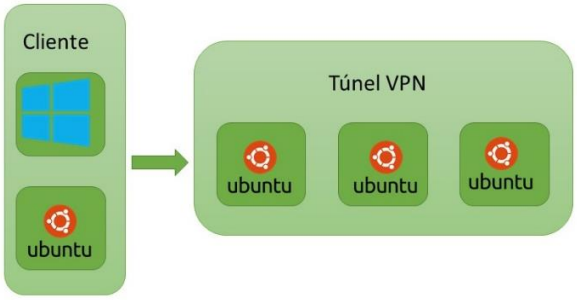

Figura 27 Cliente Windows/Ubuntu y túnel

5. Manual de Usuario

5.1. Requisitos del sistema

Como primer punto debemos distinguir la posibilidad de que el usuario que esté utilizando el software Persona Anonycloud, pueda instalar dicho software en una maquina Windows o en una máquina con Ubuntu/ AMI Linux. Como podemos ver en la figura 27.

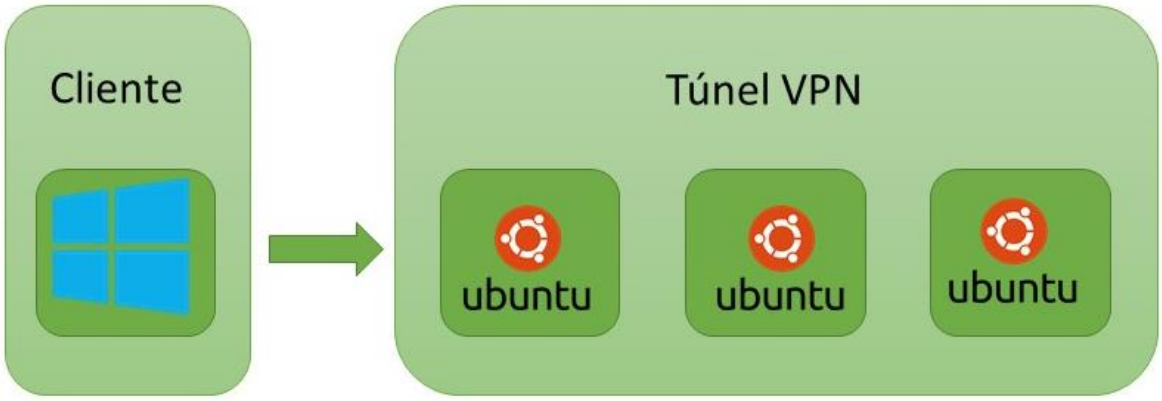

Figura 28 Cliente y servidor

Por tanto el usuario necesita de lo siguiente:

- Una máquina física con Windows.
- Una subscripción a un proveedor de máquinas virtuales en internet o bien unas máquinas físicas situadas en distintos puntos.

5.2. Simbología

Para representar el estado de las máquinas, se ha optado por representar a través del icono que describe cada proveedor, la situación de cada máquina, Lista para su uso o No disponible. Los iconos son los siguientes:

Amazon Web Services


Microsoft Azure


Máquinas propias


5.3. Instrucciones de instalación

5.3.1. Sistemas Windows

Dividiremos el proceso en dos partes:

1- Como primer paso, procederemos a la descarga del software cliente de Softether en la siguiente dirección:

SoftEther VPN Client

2- Por otro lado, ejecutaremos nuestro ejecutable de Personal AnonyCloud.

5.4. Iniciando la aplicación

Al iniciar la aplicación encontraremos la siguiente interfaz:

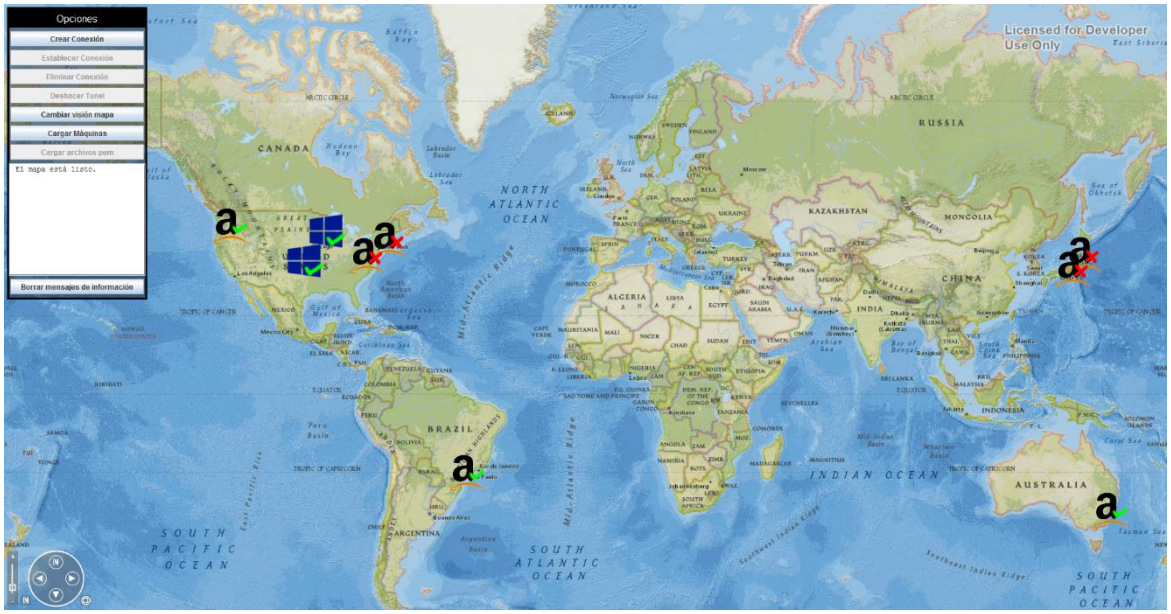

Figura 29 Interfaz principal

La aplicación cuenta con las opciones Crear Conexión, Establecer Conexión, Eliminar Conexión, Deshacer túnel, Cambiar visión mapa, Cargar Máquinas y Cargar archivos pem. Algunas de estas opciones inicialmente están desactivadas pero se van habilitando según se vayan usando las opciones disponibles.

Para obtener esta interfaz, la aplicación realiza antes lo siguiente:

Comprueba el estado de todas las máquinas que se leen del fichero inicial por defecto.

Si la máquina presenta algún tipo de problema, se mostrará el mensaje: Ha surgido un problema con la máquina y a continuación indica la IP de la máquina. Si la máquina no tiene ningún problema se mostrará: Máquina activa seguido del nombre de la máquina y de su IP. Las máquinas que han tenido algún problema aparecerán en la interfaz con un aspa rojo en el icono y las máquinas que se encuentran activas tendrán un tick verde junto al icono.

```
Ha surgido un problema con la maquina: 54.204.197.252
Ha surgido un problema con la maquina: 54.211.6.17
Ha surgido un problema con la maquina: 52.26.210.60
Ha surgido un problema con la maquina: 52.64.112.140
Maquina activa con nombre: ec2-54-207-119-72.sa-east-1.compute.amazonaws.com y direccion IP: 54.207.119.72
Maquina activa con nombre: albertovm1.cloudapp.net y direccion IP: 191.236.93.186
Maquina activa con nombre: albertovm2.cloudapp.net y direccion IP: 191.236.91.65
Ha surgido un problema con la maquina: 54.238.6.243
Ha surgido un problema con la maquina: 54.178.17.164
```

Figura 30 Salida por consola iniciando

Y a continuación se obtienen las coordenadas de cada máquina mediante el uso de un web service y una cache, la cual se usa para cuando falla el web service y permite que se pueda seguir usando la aplicación sin depender de este.

```
Current Element :Response
IP: 54.211.6.17
Codigo Pais : US
Pais : United States
Codigo Region : VA
Region : Virginia
Latitud: 39.044
Longitud : -77.488
Azure
Root element :Response
-----------------------------

Current Element :Response
IP: 191.236.93.186
Codigo Pais : US
Pais : United States
Codigo Region :
Region :
Latitud: 38
Longitud : -97
Azure
Root element :Response
-----------------------------

Current Element :Response
IP: 191.236.91.65
Codigo Pais : US
Pais : United States
Codigo Region :
Region :
Latitud: 38
Longitud : -97
```

Figura 31 Información de las máquinas

5.5. Cargar Máquinas

Para añadir las máquinas que el usuario posee en los proveedores de la nube, Amazon o Azure, o las máquinas propias debe realizar los siguientes pasos:

Primero, pulsar el botón Cargar Máquinas. Aparecerá una nueva ventana para seleccionar el fichero de máquinas que desee y solo podrá seleccionar un archivo cada vez que quiera cargar nuevas máquinas. Para continuar, debe seleccionar el botón abrir.

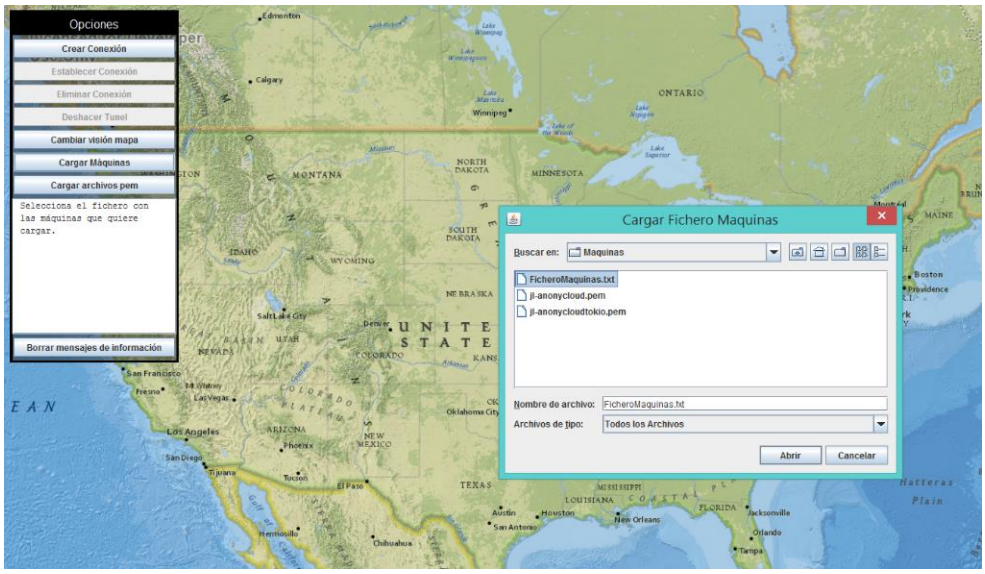

Figura 32 Cargando maquinas.txt

Si las máquinas se han cargado correctamente y están activas, aparecerán de la siguiente manera:

Figura 33 Máquinas disponibles

En este caso, todas las máquinas nuevas que se han cargado están activas pero puede suceder que se haya cargado correctamente el fichero y se muestren máquinas inactivas:

Figura 34 Máquinas inactivas

Una vez cargadas las nuevas máquinas, se habilitará el botón para cargar los archivos .pem de las nuevas máquinas. Puede cargar los ficheros en cualquier momento, no tiene por qué ser inmediatamente después de cargar las máquinas ni cargar todos los ficheros a la vez. Puede crear conexiones, deshacer conexiones, cargar un nuevo fichero de máquinas o cambiar la visión del mapa base sin tener que cargar los archivos pem. Para cargar estos archivos tiene que pulsar el botón Cargar archivos pem.

Puede seleccionar un solo archivo:

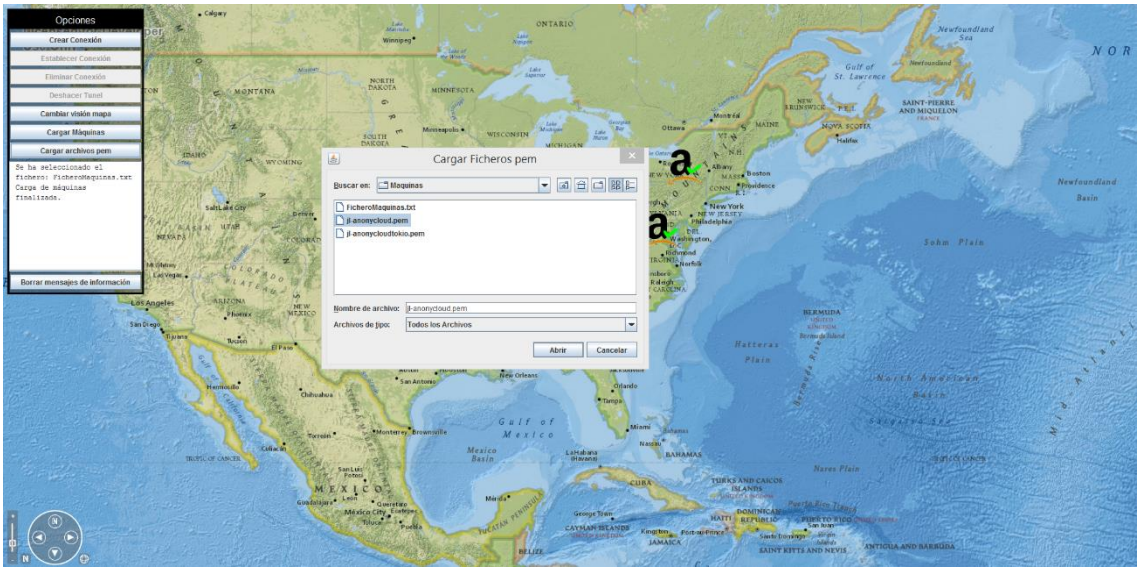

Figura 35 Seleccionando un único archivo

O puede seleccionar varios a la vez, siempre y cuando todos los archivos estén en la misma carpeta:

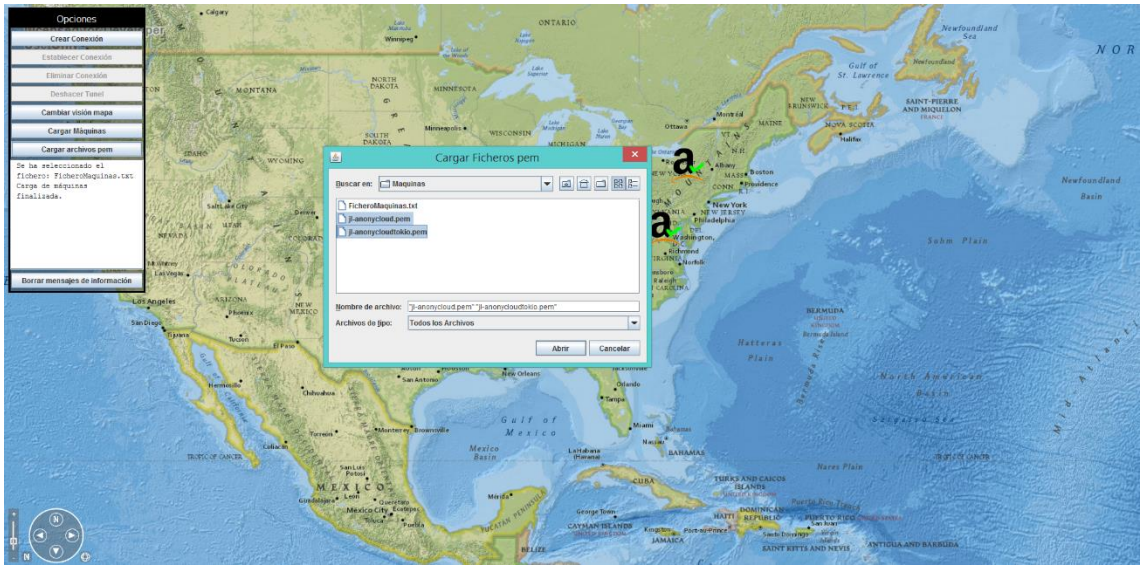

Figura 36 Seleccionando varios archivos

5.6. Crear Túnel

Para crear un nuevo túnel con las máquinas disponibles tiene que pulsar el botón Crear conexión. Pulse con el ratón sobre las máquinas que quiera conectar y según vaya pulsando sobre ellas se irá dibujando una línea que las conecta. Para terminar de dibujar una conexión, simplemente pulse con el botón derecho del ratón en cualquier parte del mapa y se finalizará el dibujo de la conexión.

Figura 37 Dibujando túnel

En la ventana que aparece en la interfaz, se muestra la información sobre las máquinas que se van conectando en cada momento y sobre los errores que se pueden producir a la hora de dibujar el túnel, como puede ser intentar conectar una máquina que se encuentra activa con una que está desactivada, o intentar unir una máquina con ella misma.

Mientras se están conectando las máquinas, siempre se está comprobando que están activas y disponibles para ser conectadas.

```
Maquina activa con direccion IP: 191.236.93.186
Maquina activa con direccion IP: 191.236.91.65
Maquina activa con direccion IP: 191.236.91.65
Maquina activa con direccion IP: 191.236.93.186
Maquina activa con direccion IP: 191.236.93.186
Maquina activa con direccion IP: 54.211.6.17
Maquina activa con direccion IP: 191.236.91.65
Maquina activa con direccion IP: 191.236.93.186
Maquina activa con direccion IP: 191.236.93.186
Maquina activa con direccion IP: 54.211.6.17
Maquina activa con direccion IP: 54.211.6.17
Maquina activa con direccion IP: 54.204.197.252
Maquina activa con direccion IP: 54.204.197.252
Maquina activa con direccion IP: 54.238.6.243
Maquina activa con direccion IP: 54.238.6.243
Maquina activa con direccion IP: 54.178.17.164
```

Figura 38 Salida por consola de la consulta del estado de las máquinas

Una vez que termine de dibujar la conexión, se muestra por la ventana de información la IP a la que tiene que conectarse cuando establezca una conexión y se habilitarán las opciones de Establecer Conexión entre las máquinas seleccionadas y Deshacer el túnel dibujado. Para poder dibujar un nuevo túnel, es necesario que elimine el que haya creado previamente ya que si no lo elimina no podrá crear ninguna conexión nueva.

Figura 39 IP facilitada por PA para conectar el túnel

5.7. Establecer Conexión

Para establecer una conexión, debe descargar e instalar el software SoftEther VPN Client si no lo tiene aún descargado.

Descarga SoftEther VPN Client:

http://www.softether-download.com/en.aspx?product=softether

Para iniciar la descarga, en el apartado de Select Software hay que seleccionar la única opción que hay, que es SoftEther VPN (Freeware), y en el apartado Select Component seleccionar la opción SoftEther VPN Client. Cuando se selecciona esta opción aparece un nuevo apartado que es Select Plaform y se seleccionará la plataforma Windows. Por último, cuando se selecciona Windows, aparece de nuevo otro apartado que es Select CPU y aquí solo hay una opción posible que es Intel (x86 and x64).

Finalmente, seleccionar la versión SoftEther VPN Client 4.17 y guardar el archivo.

Instalación SoftEther VPN Client:

Ejecutar el archivo que se ha descargado y seguir los siguientes pasos:

Figura 40 Instalando SoftEther I

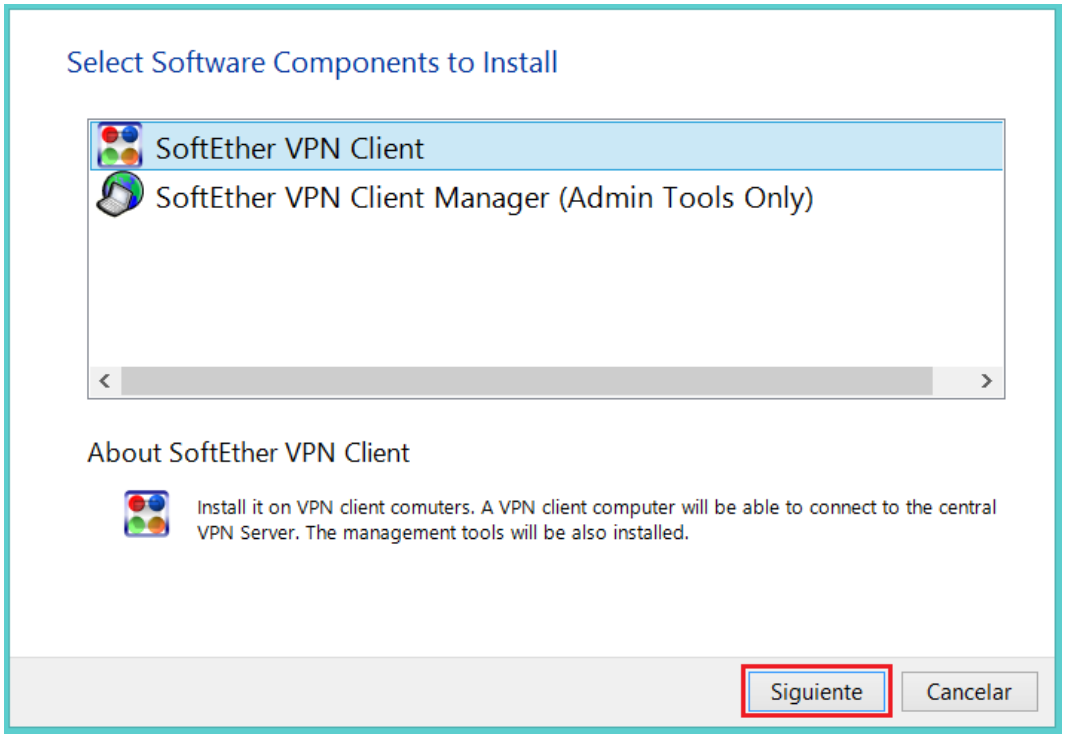

Figura 41 Instalando SoftEther II

Figura 42 Instalando SoftEther III

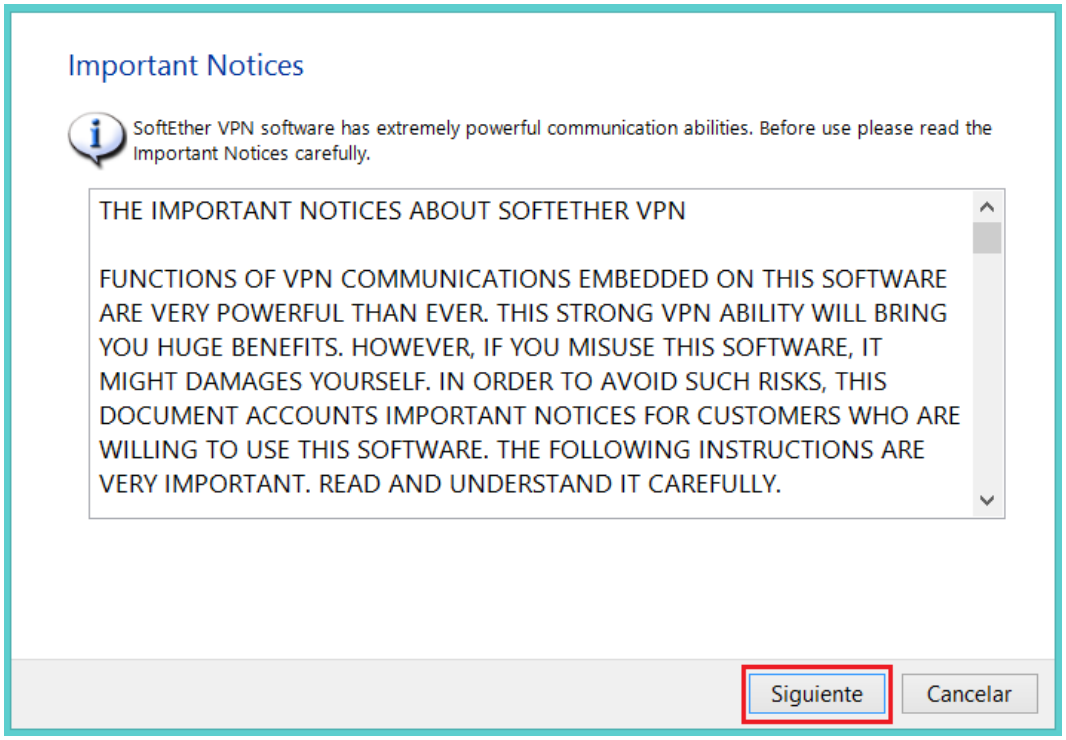

Figura 43 Instalando SoftEther IV

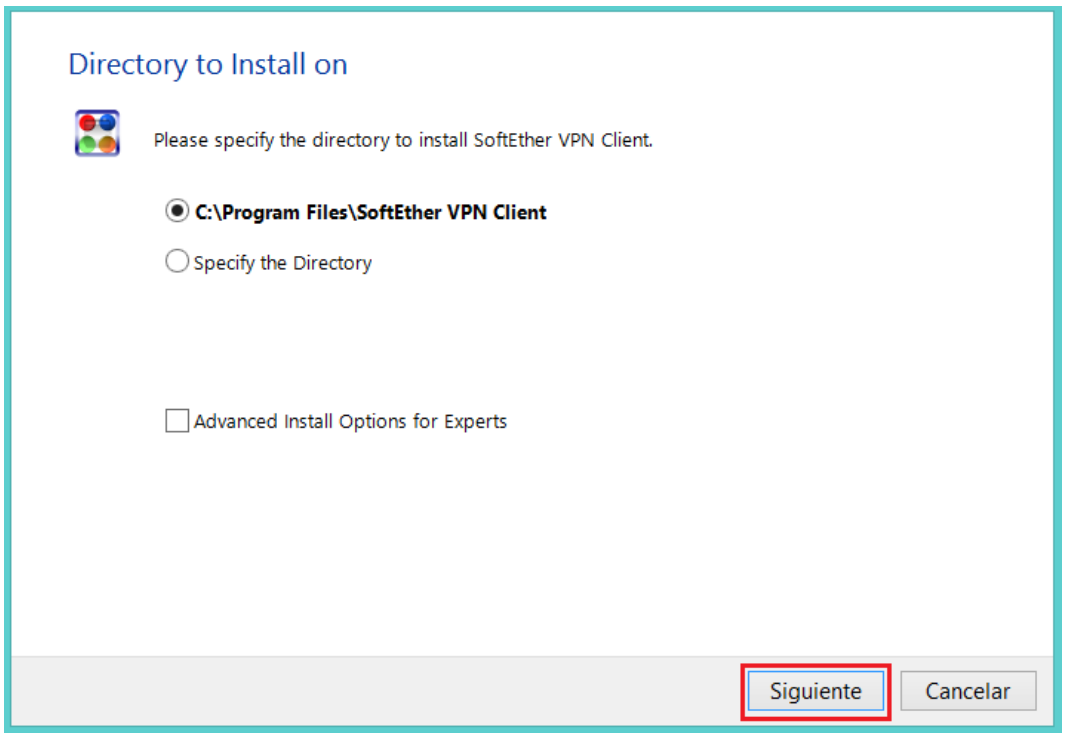

Figura 44Instalando SoftEther V

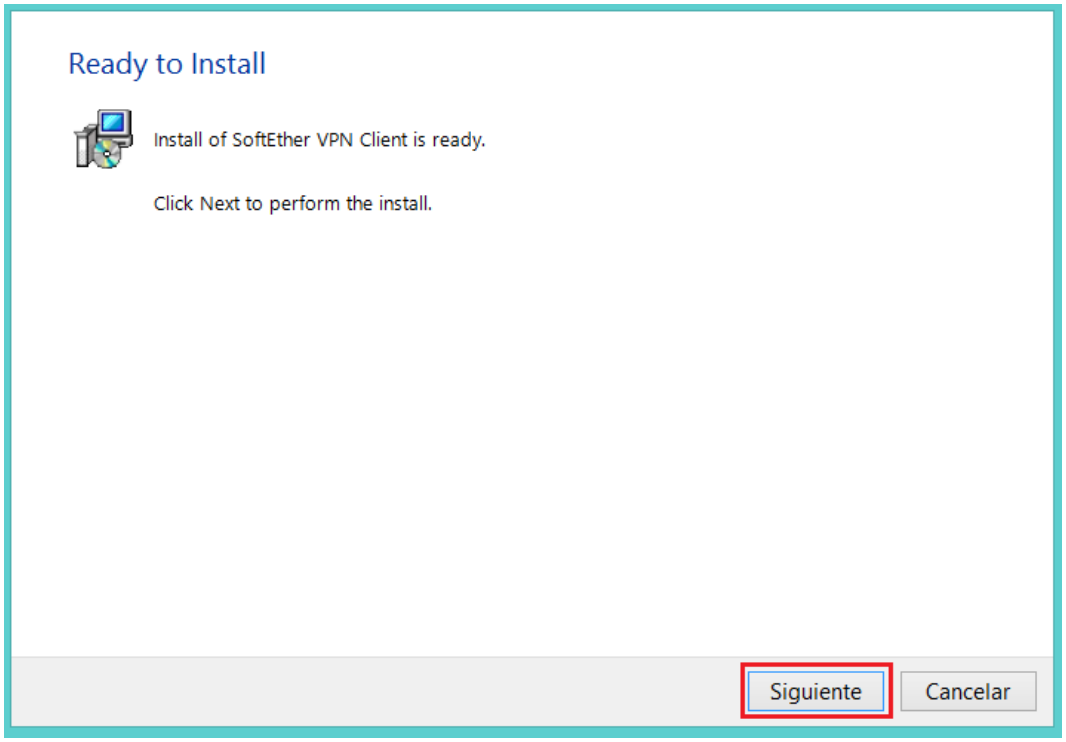

Figura 45 Instalando SoftEther VI

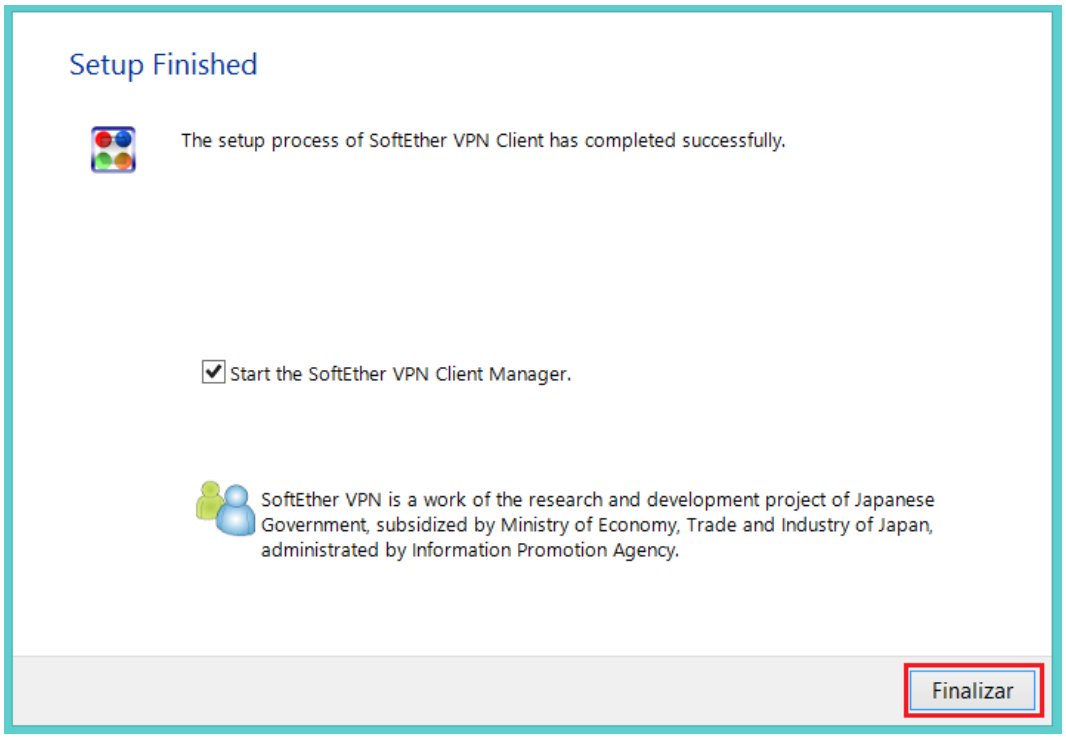

Figura 46 Instalando SoftEther VII

Configuración SoftEther Client:

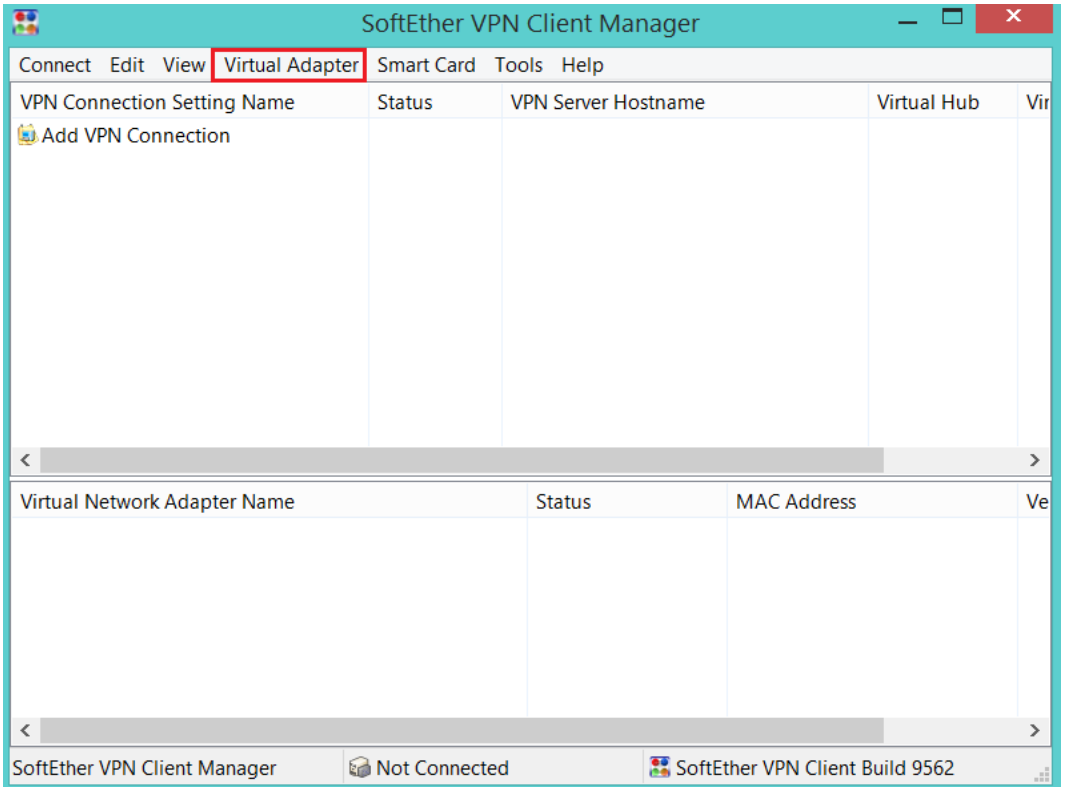

Figura 47 Instalando SoftEther VIII

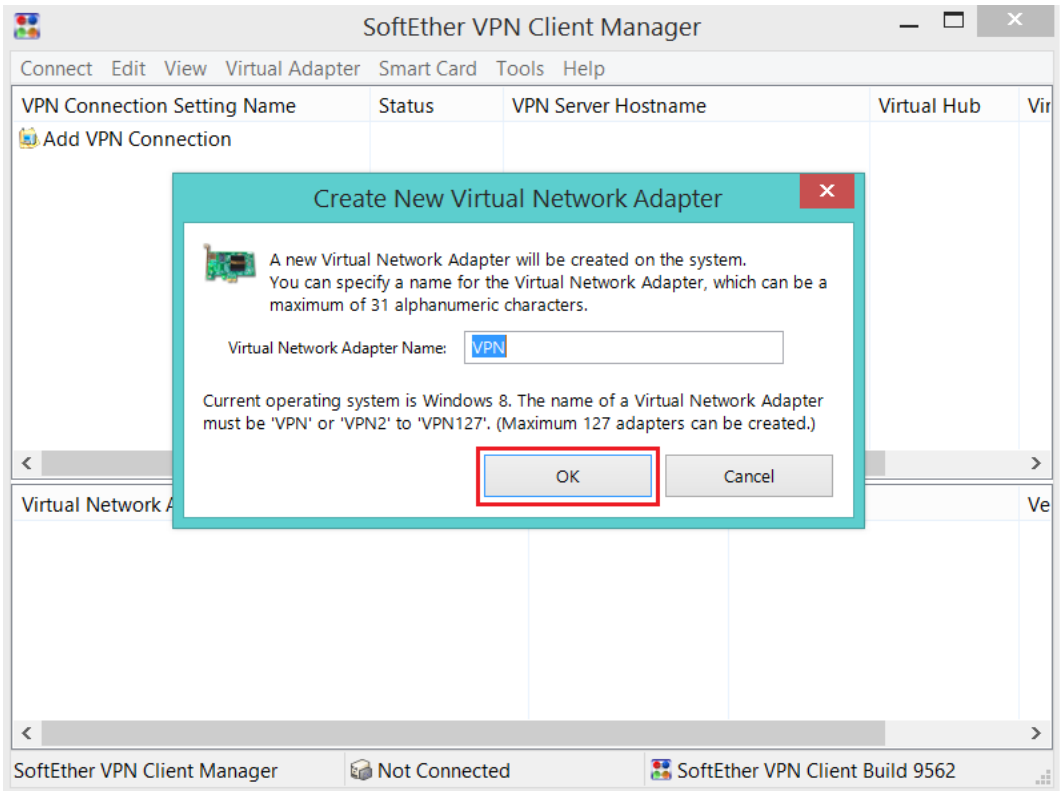

Figura 48 Instalando SoftEther IX

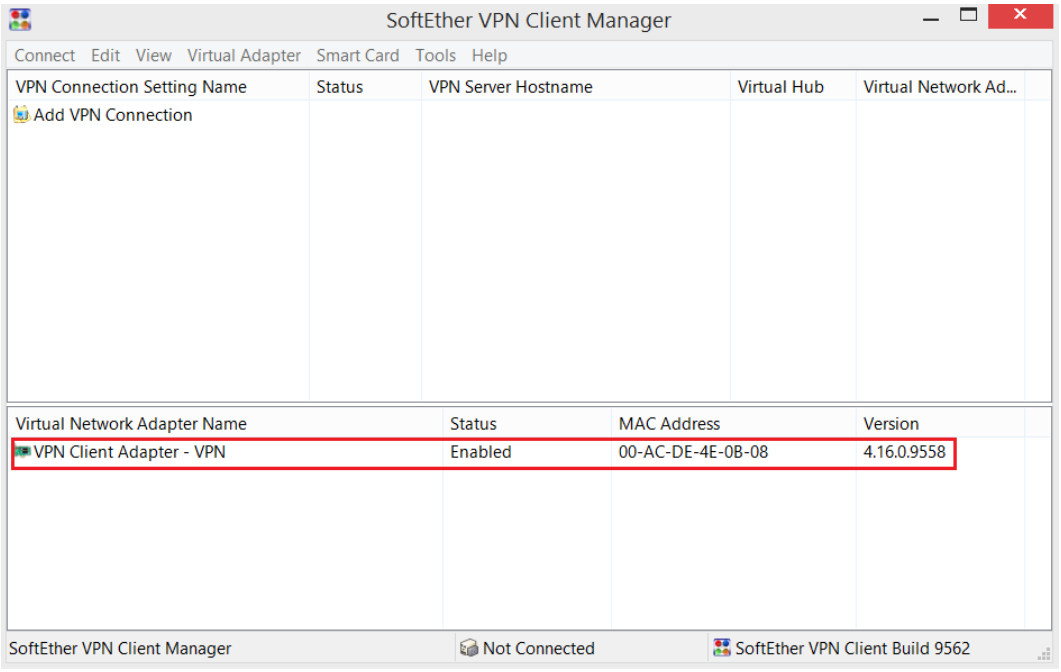

Figura 49 Instalando SoftEther X

Establecer la conexión:

Para establecer la conexión de las máquinas que se han conectado, en la interfaz de Personal Anonycloud tendrá que pulsar en el botón Establecer conexión. A partir de aquí comienza un proceso que toma unos minutos, en los que se descarga el software, se instala y se realizan todas las conexiones entre las máquinas del túnel de manera automática. Recordar que a la hora de establecer una conexión con sus máquinas propias, tiene que seleccionar los ficheros pem necesarios de las máquinas que están seleccionadas en el túnel para poder establecer la conexión.

Figura 50 Estableciendo conexión

A continuación, vaya a SoftEther VPN Client y pulse Connect -> New VPN Connection Setting y aparecerá la siguiente pantalla:

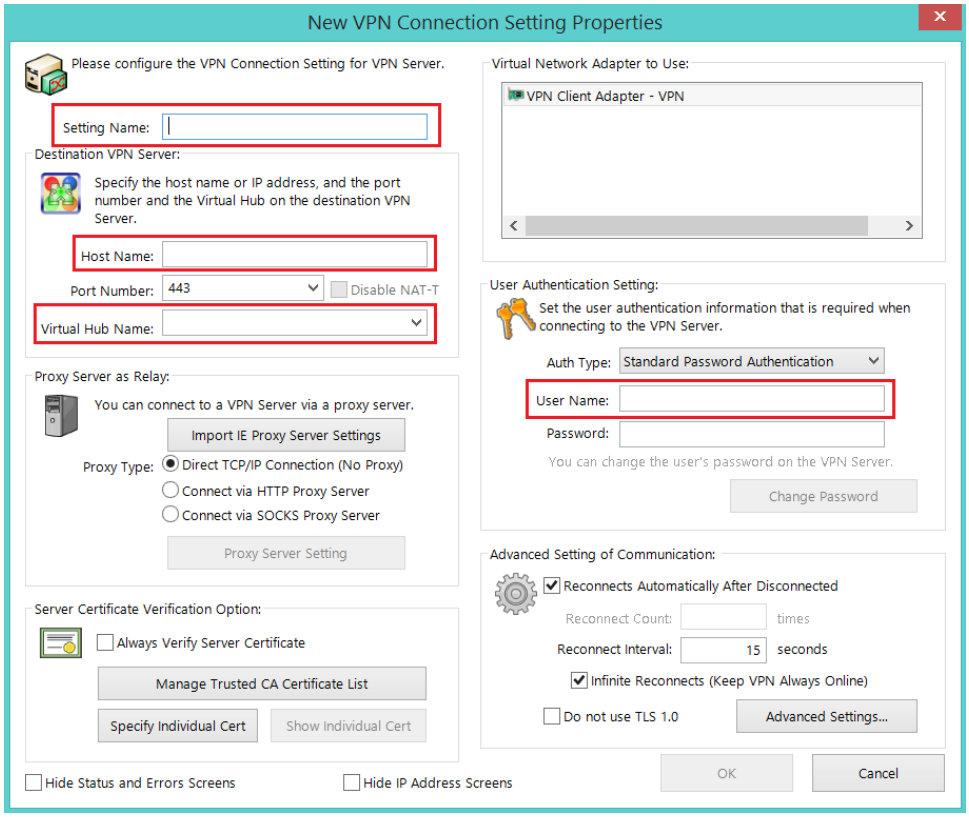

Figura 51 Rellenando datos de conexión en SoftEther

Los campos marcados son los que hay que completar para poder establecer la conexión. En Setting Name ponga el nombre que desee, en Host Name debe poner la IP que se mostraba en la ventana de información, una vez que ponga la IP, en Virtual Hub Name saldrá DEFAULT, el cual tiene que seleccionar, y finalmente seleccionar Auth Type como Anonymous Authentication y poner el User Name, en el que tendrá que poner USER que le permitirá conectarse sin necesidad de una contraseña.

Cuando pulse OK, saldrá la siguiente pantalla:

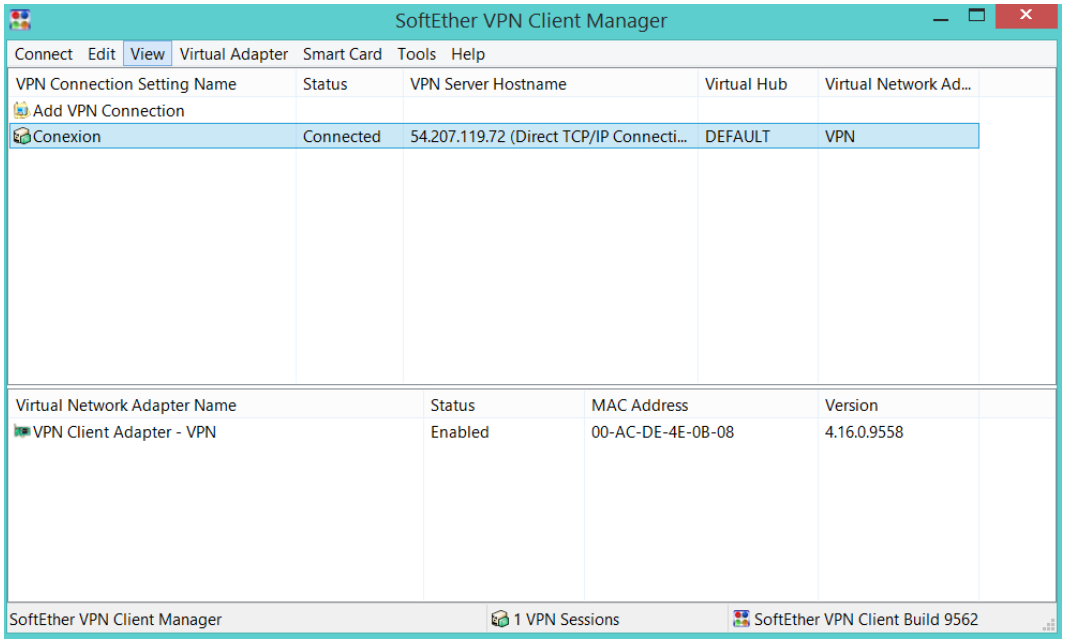

Figura 52 Listado de conexiones VPN en SoftEther

Si la nueva configuración aparece offline, pulse sobre ella con el botón derecho del ratón y saldrá la opción Connect, pulse aquí y finalmente se establecerá la conexión.

Cuando se establezca la conexión, SoftEther mostrará en una ventana su nueva IP, pero como se cierra rápidamente y quizás no le dé tiempo a verla, puede consultar su IP en la siguiente página:

http://www.cualesmiip.com/

Y con el ejemplo mostrado se obtiene la siguiente IP:

Figura 53 Resultado de consulta de la IP

Es la IP de la máquina de Azure que habíamos seleccionado en último lugar al dibujar el túnel. Se puede comprobar que esta IP corresponde a esta máquina en la sección Iniciando la aplicación, donde se muestran las IPs de todas las máquinas usadas en los ejemplos.

5.8. Deshacer Túnel

Esta opción se habilitará cuando haya creado una nueva conexión previamente. Cuando pulse Deshacer túnel, desaparecerá de la pantalla la conexión que tuviese hecha y la aplicación quedará tal y como estaba al inicio. Después de deshacer el túnel, ya podrá crear, si lo desea, una nueva conexión.

5.9. Eliminar Túnel

Esta opción eliminará el túnel que se haya establecido previamente, borrando de la interfaz la conexión que se ha establecido entre las máquinas, elimina los túneles establecidos entre las máquinas que se habían seleccionado y limpia los archivos que se han usado para establecer los túneles de todas las máquinas seleccionadasl túnel. Cuando elimine el túnel, debe desconectar también la configuración creada de SoftEther. Esto lo puede hacer pulsando con el botón derecho sobre esta configuración y pulsar Disconnect.

5.10. Encolar máquina a túnel ya creado

Con el túnel ya creado, podemos encolar una nueva máquina a nuestro túnel.

Basta con pulsar en el botón “Encolar máquina a túnel”, y uniremos la máquina que deseemos al igual que hemos creado el túnel primero. Haciendo clic en el extremo y en la nueva máquina.

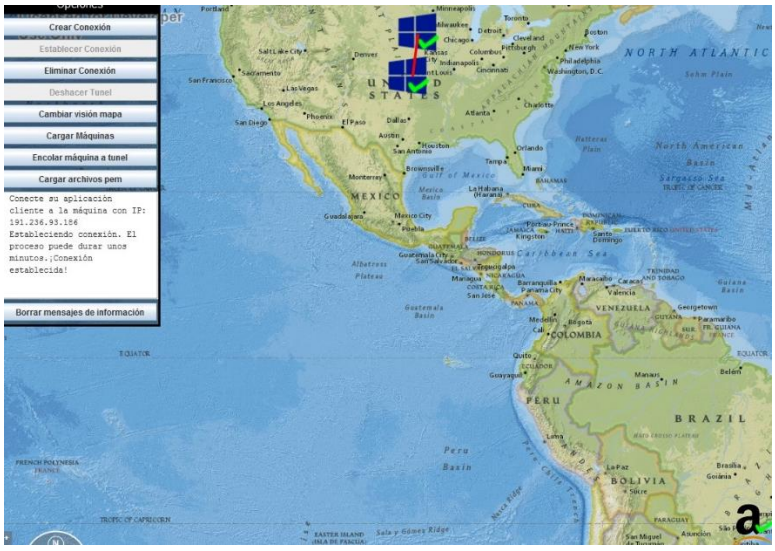

Figura 54 Encolando una nueva máquina Amazon a nuestro túnel VPN

Después de haber realizado el trazado del túnel entre la máquina que deseamos añadir y nuestro túnel, el resultado es el siguiente:

Figura 55 Resultado de encolar máquina al túnel

5.11. Activar o desactivar Máquinas

Podrá activar o desactivar las máquinas pulsando con el botón derecho sobre la máquina que quiera editar. Si hay una conexión creada no se podrá editar ninguna de las máquinas.

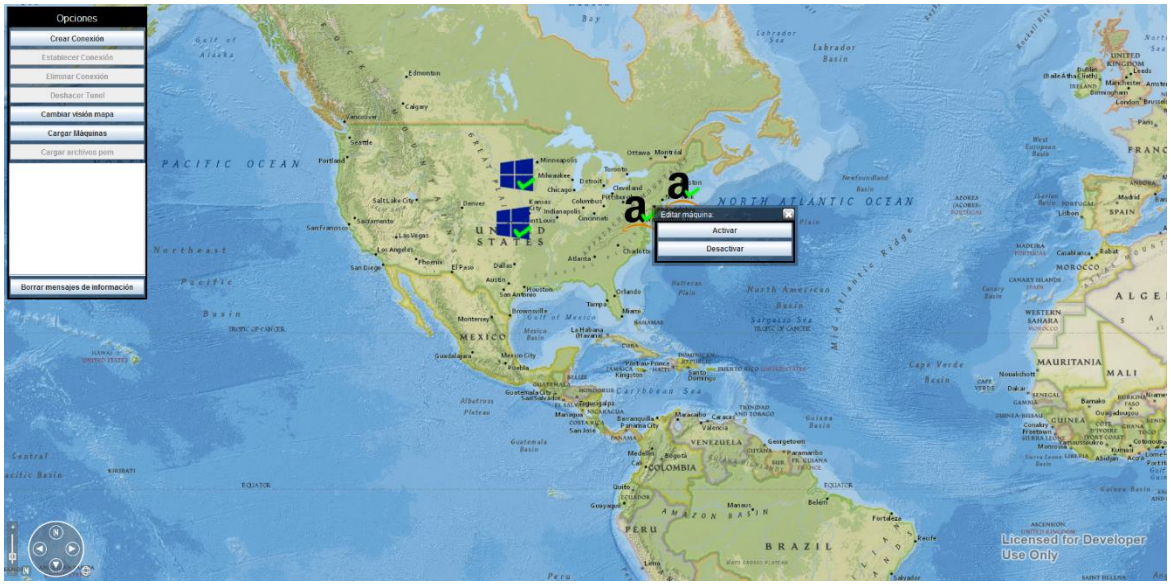

Figura 56 Ventana activación o desactivación de cada máquina

Figura 57 Resultado de desactivación con el menú

5.12. Cambiar visión mapa

En cualquier momento podrá cambiar el mapa base que se muestra en la aplicación. Haciendo clic en el botón “Cambiar visión mapa” podremos acceder a un abanico de 8 mapas diferentes. Por defecto esta puesto el mapa National Geographic, pero tiene las siguientes opciones:

5.11.1. Gris claro

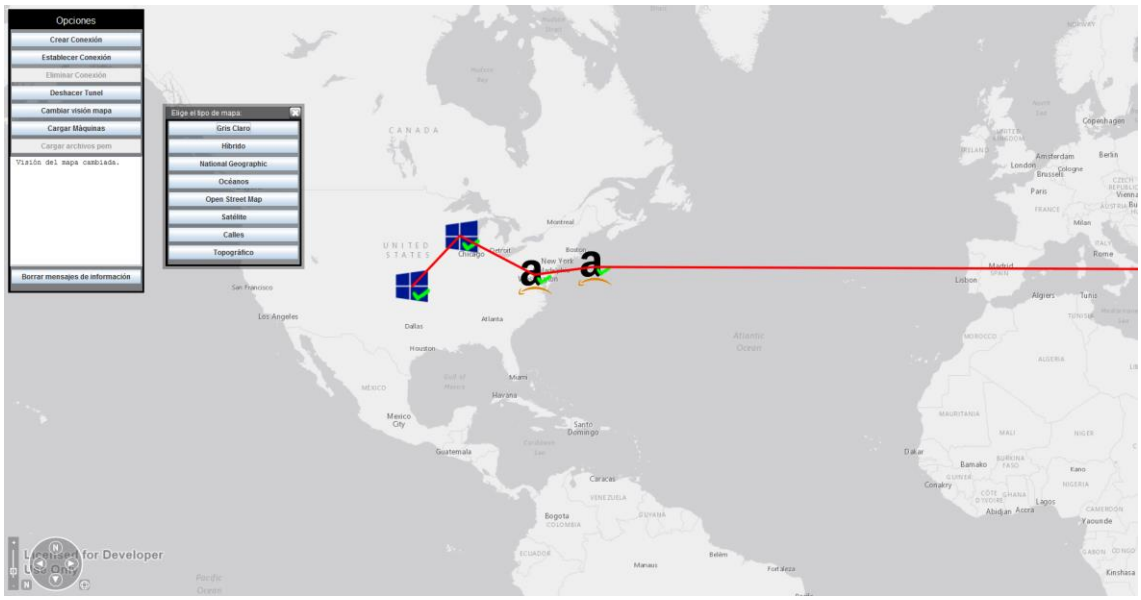

Figura 58 Mapa gris claro

5.11.2. Híbrido

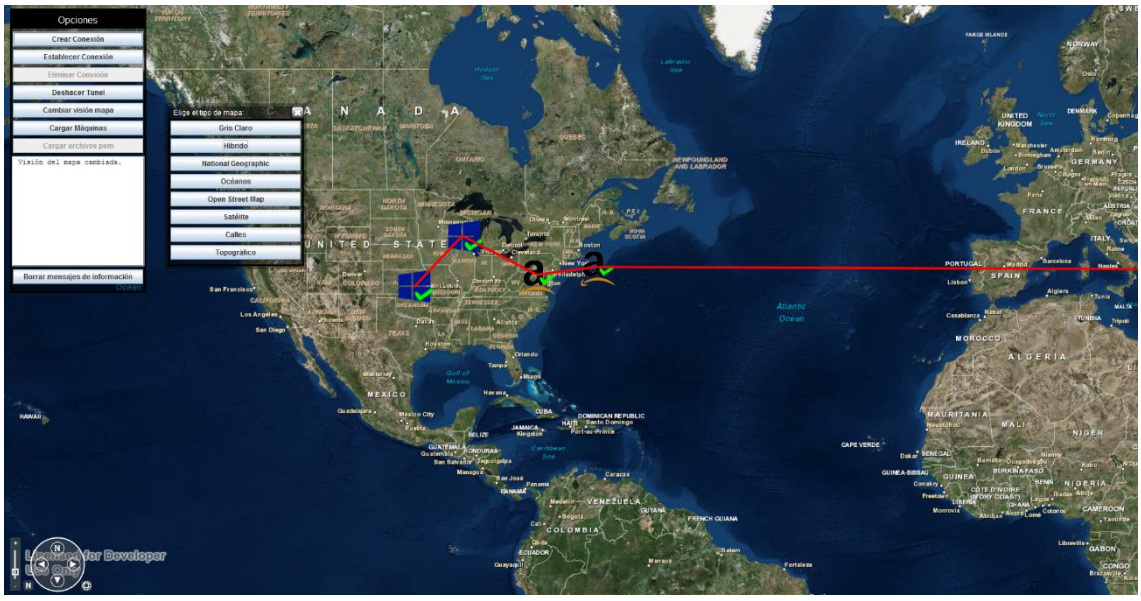

Figura 59 Mapa híbrido

5.11.3. Océanos

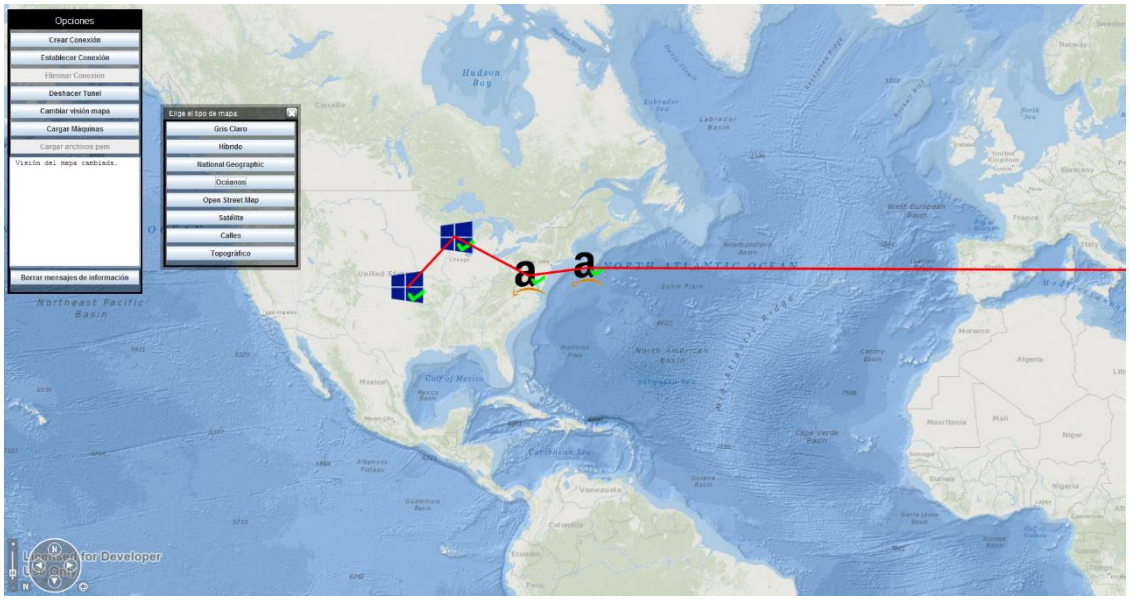

Figura 60 Mapa océanos

5.11.4. Open Street Map

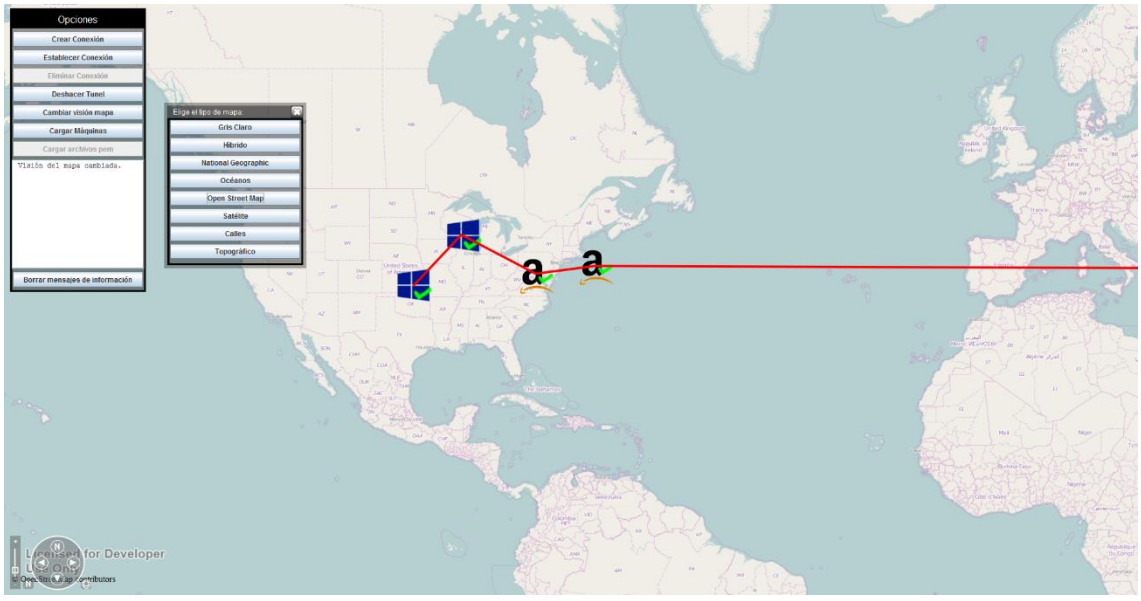

Figura 61 Mapa open street map

5.11.5. Satélite

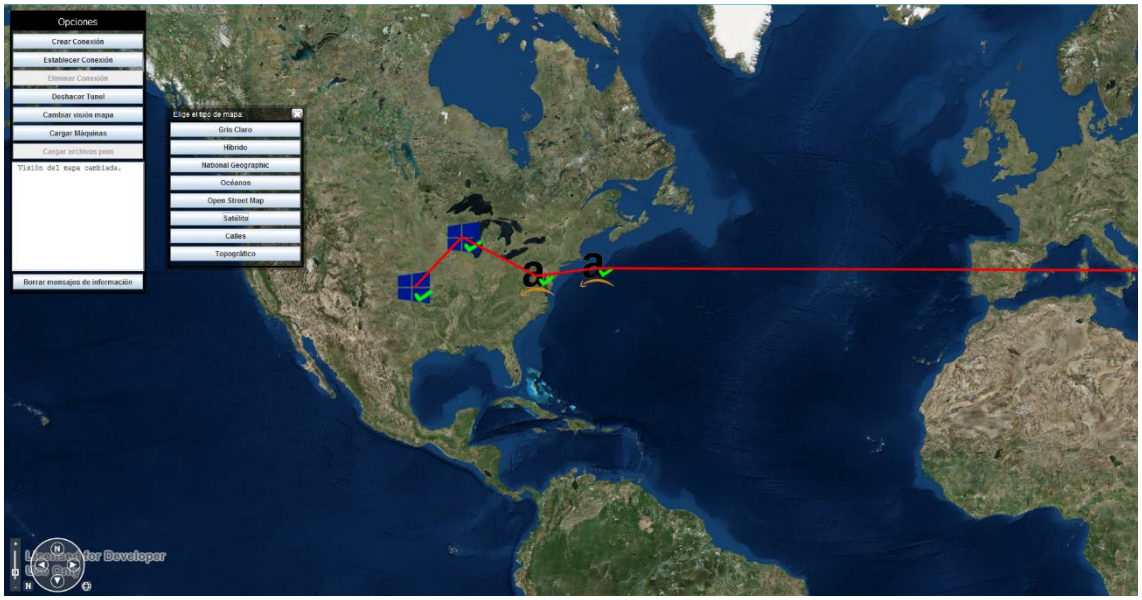

Figura 62 Mapa satélite

5.11.6. Calles

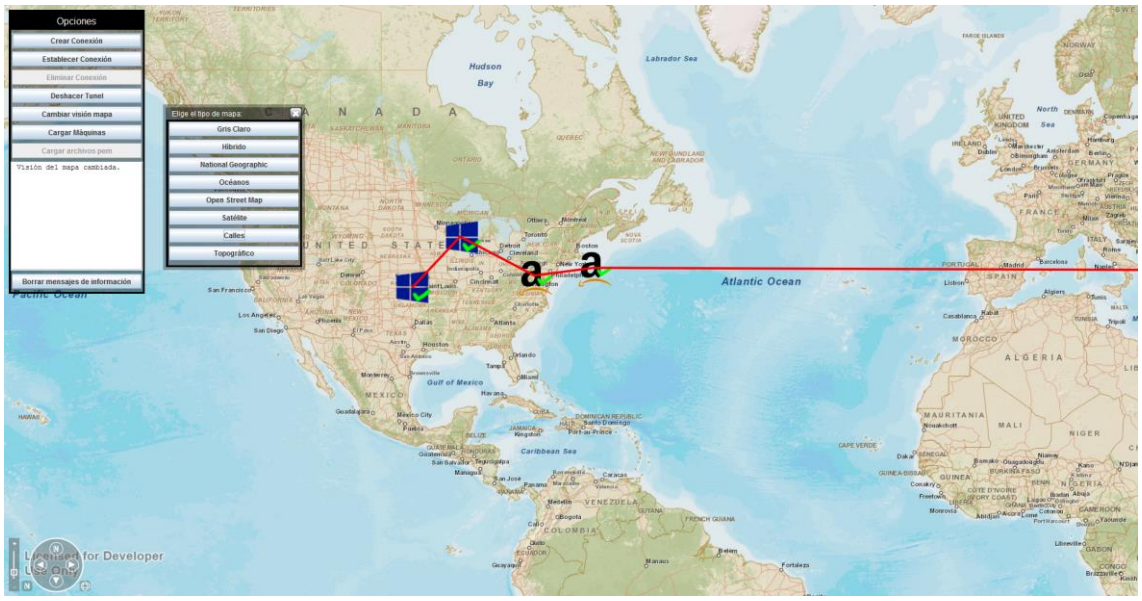

Figura 63 Mapa calles

5.11.7. Topográfico

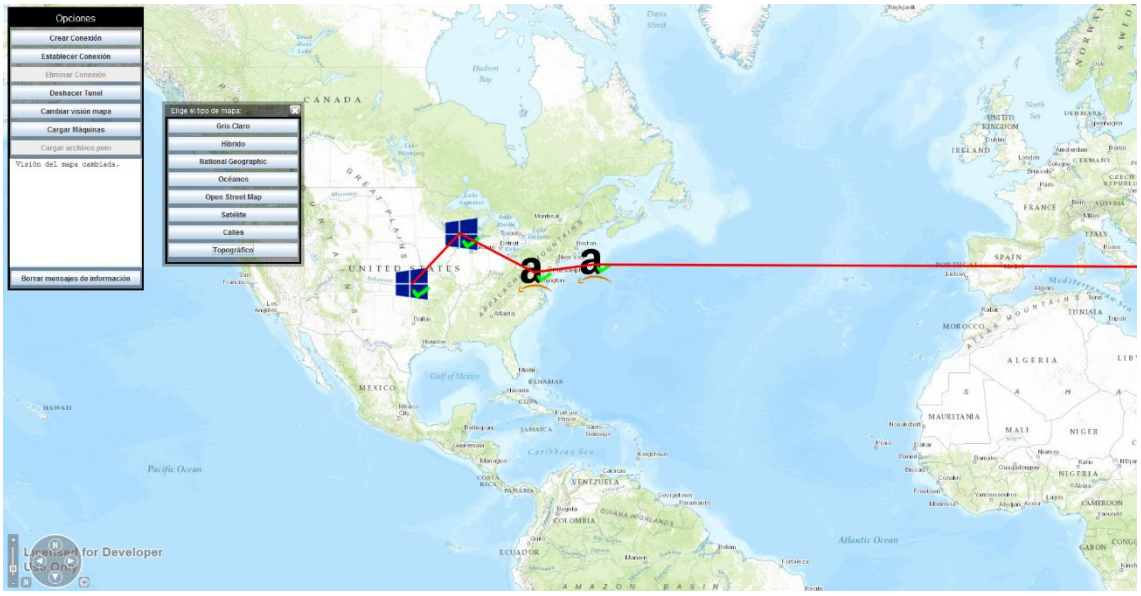

Figura 64 Mapa topográfico

5.11.8. National Geographic (Por defecto)

Figura 65 Mapa National Geographic

6. Bibliografía

SoftEther VPN Project. Disponible en: http://www.softether.org/

ArcGIS. Disponible en: http://www.arcgis.com/

ArcGIS. ¿Qué es ArcGIS? Disponible en: http://resources.arcgis.com/es/help/getting-started/articles/026n00000014000000.htm

ArcGIS. Representación y modelado de un GIS. Disponible en: http://resources.arcgis.com/es/help/getting-started/articles/026n0000000r000000.htm

ArcGIS. Manual SDK para Java . Disponible en: https://developers.arcgis.com/java/guide/guide.htm

Jcraft, Desarrollado de JSch. http://www.jcraft.com/jsch/

N. I. o. S. Technology, "The NIST definition of Cloud Computing," Special Publication 800- 145, National Institute of Standards and Technology, July 2011. Disponible en http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf

Figura 1.Virtual Private Network. Disponible en: http://www.hcltech.com/sites/default/files/rise-of-clouds.jpg

Figura 14. Cloud as a Service, Saas, Iaas, Paas. Disponible en: http://cloudcelebrity.files.wordpress.com/2011/11/cloud_20.png

Figura 15. Representación de GIS Wolrd Model. Disponible en: http://www.in.gov/gis/images/Capture9.PNG

Figura 16. Esquema de funcionamiento de Servicio Web. Disponible en: http://help.sap.com/saphelp_mdm550/helpdata/en/45/018c03166a0486e10000000a155369/frameset.htm